Estudo Comparativo dos Aspectos de Segurança em Redes WWAN, WLAN e WPAN

Daniella Arruda Franceschinelli

Trabalho Final de Mestrado Profissional

Instituto de Computação
Universidade Estadual de Campinas

Estudo Comparativo dos Aspectos de Segurança em Redes WWAN, WLAN e WPAN

Daniella Arruda Franceschinelli

05 de Dezembro de 2003

Banca Examinadora:

- **Prof. Dr. Ricardo Dahab (Orientador)**
  IC - Unicamp
- **Prof. Dr. Paulo Lício de Geus**
  IC - Unicamp
- **Prof. Dr. Omar Branquinho**
  PUC - Campinas
- **Prof. Dr. Guido Araújo (Suplente)**
  IC - Unicamp

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Franceschinelli, Daniella Arruda

F844e Estudo comparativo dos aspectos de segurança em redes WWAN, WLAN e WPAN/ Daniella Arruda Franceschinelli -- Campinas, [S.P. :s.n.], 2003.

Orientador : Ricardo Dahab.

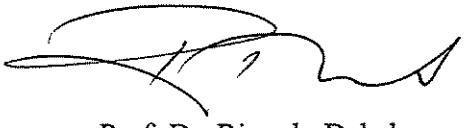
Trabalho final (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Computação.

1. Redes de computação – Medidas de segurança. 2. Sistemas de computação sem fio. I. Dahab, Ricardo. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Estudo Comparativo dos Aspectos de Segurança em Redes WWAN, WLAN e WPAN

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigido e defendido por Daniella Arruda Franceschinelli e aprovado pela Banca Examinadora.

Campinas, 05 de Dezembro de 2003.



Prof. Dr. Ricardo Dahab
(Orientador)

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Computação na área de Engenharia de Computação

TERMO DE APROVAÇÃO

Trabalho Final Escrito defendido e aprovado em 05 de dezembro de 2003, pela Banca Examinadora composta pelos Professores Doutores:

Prof. Dr. Omar Carvalho Branquinho
PUC-CAMPINAS

Prof. Dr. Paulo Lício de Geus
IC - UNICAMP

Prof. Dr. Ricardo Dahab
IC - UNICAMP

Aos meus pais,

com muita gratidão

Agradecimentos

A Deus pela minha vida, saúde e trabalho;

À Santa Rita de Cássia pela ajuda na superação dos momentos difíceis;

À Marcos pelo apoio e paciência;

À minha família que sempre soube compreender as minhas ausências nos churrascos e almoços dominicais;

Ao meu orientador Ricardo, que sempre me recebeu com sorrisos e me deu bastante ânimo na condução deste trabalho;

À banca examinadora composta pelos professores Omar Branquinho e Paulo Lício de Geus, pela leitura cuidadosa e sugestões feitas.

À direção da Faculdade Prudente de Moraes, principalmente o Prof. Luiz Roberto que me liberou de horas preciosas de trabalho para participar das reuniões com o orientador e para elaborar este trabalho;

Aos demais colegas da Faculdade Prudente de Moraes que sempre me deram apoio e estímulo para não desistir e ouviram com paciência (nem sempre!) as minhas lamentações e preocupações;

A todos os usuários com quem já trabalhei nestes anos. Com certeza muito do que aprendi com eles está neste trabalho.

Resumo

O surgimento e as evoluções das tecnologias *wireless* proporcionaram maior interesse pela mobilidade, que contribuíram no avanço da comunicação móvel.

A crescente utilização das redes sem fios, por um lado, gerou novos negócios nos serviços de comunicação pessoal, mas por outro, trouxe novos problemas relacionados à segurança, tais como a maior exposição dos meios de transmissão e maior complexidade nos processos de autenticação.

Este trabalho apresenta inicialmente uma visão geral dos sistemas de redes sem fios GSM, 802.11 e *Bluetooth*, destacando suas arquiteturas, componentes, funcionalidades e benefícios. Esta apresentação inicial serve como base para discutir os aspectos de segurança nessas redes sem fios e compará-los com outras tecnologias existentes no mercado, especialmente quanto aos requisitos de autenticação, confidencialidade, disponibilidade e privacidade.

Abstract

The constant evolution of wireless technologies have prompted an increasing interest for mobile computing in general, which in turn have contributed to advancements in mobile communication.

If, on one side, wireless networks opened the possibilities for personal service businesses, they also exposed a whole new range of serious security issues such as greater exposure of the communication media and more complex, and thus more error prone, authentication procedures.

This work presents, initially, a broad overview of wireless network systems, specifically GSM, 802.11 and Bluetooth, highlighting its architectures, components, functionalities and positive aspects. This overview is then used as a basis for discussing their security aspects and for comparing them with other technologies available in the market, specially with regard to authentication, confidentiality and availability.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

O desenvolvimento do capitalismo mudou a realidade do mundo econômico, e um exemplo desse novo cenário é, sem dúvida, a globalização – movimento que ganhou turbinas com o avanço das telecomunicações e a convergência das tecnologias. Nessa mesma esteira, destaca-se a popularização da Internet, grande responsável por inúmeras mudanças no mundo nos últimos anos, onde um simples clique torna a informação disponível em todos os lugares.

Porém, mesmo com a popularização da Internet, o número de usuários ainda é pequeno na maioria dos países, devido a pouca oferta de linhas telefônicas convencionais, o preço dos computadores, o custo do treinamento na utilização dos computadores, etc.

Com o objetivo de elevar o número de usuários, foram criadas novas tecnologias para possibilitar o acesso à Internet sem precisar usar o computador, sendo a principal delas a tecnologia *wireless,* que permite que aparelhos móveis, como telefone celular, *palmtop*, PDA, acessem a Internet.

Os benefícios das redes móveis em relação às redes cabeadas são inúmeros, incluindo a mobilidade do usuário e a eliminação de custos de cabeamento; porém, sérios problemas de segurança são apresentados, pois as redes sem fios usam como meio de transmissão o ar, permitindo fácil acesso dos intrusos aos dados transmitidos.

Com as evoluções no mundo *wireless*, que fazem com que o interesse pela mobilidade contribua no avanço da comunicação móvel e geram novos negócios nos serviços de comunicação pessoal, a preocupação com a segurança torna-se cada vez mais importante.

Os meios sem fio, ao permitir o livre acesso, expõem o conteúdo da comunicação entre uma unidade sem fio e a rede cabeada ou mesmo entre unidades sem fio, dando ao intruso a oportunidade de invadir o ambiente como se estivesse caracterizado de assinante legítimo.

Outro problema relacionado com segurança diz respeito à mobilidade, já que um computador móvel pode se conectar a rede em diferentes locais, confiáveis ou não, pondo em dúvida se todas as mensagens enviadas pertencem à unidade móvel em questão.

Características de segurança como sigilo e controle de fraudes são necessárias para o fornecimento da proteção nesse meio de comunicação. Em princípio, estas características

poderiam ser conseguidas através da autenticação, que verifica a identidade das entidades finais do ambiente sem fio e estabelece uma chave secreta entre elas para que a comunicação siga seguramente.

O objetivo deste trabalho é realizar um estudo comparativo das tecnologias de redes *wireless* mais importantes, como GSM, GPRS e UMTS caracterizando as redes WWAN; WLAN 802.11, HiperLAN/2 e HomeRF as redes WLAN e *Bluetooth* e IrDA as WPAN, nos aspectos de segurança.

Para isto, os requisitos de autenticação, confidencialidade, disponibilidade e privacidade são abordados e avaliados.

É traçado um panorama geral dessas tecnologias, mostrando a arquitetura, os componentes e funcionalidades e seus benefícios. No tocante à segurança, além de apresentar as vantagens a elas inerentes, também são relatadas as deficiências e os mecanismos através dos quais indivíduos não autorizados poderiam acessar as informações disponibilizadas em tais redes de maneira relativamente fácil.

1.1 Organização Deste Documento

Este documento foi dividido em 8 capítulos, organizados e divididos da seguinte forma:

- **Capítulo 2 – Segurança de Redes e da Informação:** São definidos os requisitos, os problemas e os mecanismos de segurança nas redes em geral. Nesse capítulo, é introduzido um método para o desenvolvimento do processo de análise de segurança chamado I-ADD. São mostrados os princípios básicos de criptografia que deveriam ser entendidos no desenvolvimento das soluções *wireless*.
- **Capítulo 3 – Computação Móvel**: São apresentados os conceitos e características dos sistemas móveis. São mostrados os métodos de acesso para sistemas de comunicação móvel. É apresentado o termo *wireless* como uma evolução ocorrida no ambiente móvel. São abordados os sistemas de redes *wireless* WWAN, WLAN, WMAN e WPAN e suas tecnologias.
- **Capítulo 4 – Redes *Wireless* WAN:** É apresentada a evolução dos sistemas celulares. O capítulo dá destaque à tecnologia GSM, mostrando sua arquitetura e benefícios. São mostrados alguns aspectos de segurança do padrão GSM, como a autenticação, confidencialidade dos dados e do assinante, mas também seus problemas. São apresentados exemplos de ataques à tecnologia GSM.

- **Capítulo 5 – Redes *Wireless* LAN:** É examinada a tecnologia de rede local sem fio 802.11, incluindo sua arquitetura, seus benefícios e seus padrões de segurança. São apresentados os problemas de segurança com o padrão IEEE 802.11 e alguns ataques ocorridos. São propostas contra-medidas de segurança para o padrão. É apresentado o padrão 802.16 para redes metropolitanas.
- **Capítulo 6 – Redes *Wireless* PAN:** É apresentada a tecnologia de rede ad hoc *Bluetooth*, evidenciando sua arquitetura e benefícios. São mostrados os aspectos de segurança, como a autenticação, confidencialidade e os níveis de confiança, de serviço e autorização, e algumas contra-medidas relacionadas aos sistemas *Bluetooth*.
- **Capítulo 7 – Comparativo dos aspectos de segurança de outras tecnologias de redes sem fios existentes:** No capítulo, é feita uma análise comparativa de alguns aspectos, destacando a segurança, das redes GPRS e UMTS com as GSM; de HiperLAN/2 e HomeRF com WLAN 802.11 e do IrDA com o *Bluetooth*.
- **Capítulo 8 – Conclusão:** Este capítulo sintetiza as contribuições deste trabalho e apresenta as conclusões.

Capítulo 2

Segurança de Redes e da Informação

As redes podem ser definidas como sistemas nos quais os dados são armazenados e processados, através dos quais são transmitidos [LAUDON+1999]. São formadas por componentes de transmissão (cabos, ligações sem fio, satélites, encaminhadores, pontos de interconexão, nós de comutação, etc) e serviços de suporte (sistema de nomes de domínio, serviços de autenticação, por exemplo). Há uma gama crescente de aplicações e equipamentos ligados em redes, destacando-se os telefones fixos, os móveis, computadores pessoais, servidores, entre outros.

Os sistemas de computadores desempenham um papel tão crítico em empresas, governo e na vida diária, que as organizações precisam seguir regras especiais para proteger suas redes e sistemas de informações e assegurar que eles serão precisos e confiáveis.

Os sistemas de informação concentram os dados em arquivos que, potencialmente, podem ser acessados mais facilmente por um grande número de pessoas e por grupos de fora da organização. Conseqüentemente, os dados automatizados são mais suscetíveis a destruição, fraude, erro e uso indevido.

Os avanços nas telecomunicações ampliaram as vulnerabilidades. Através das redes de telecomunicações, os sistemas de informação em diferentes localidades podem ser interconectados. O potencial para acesso não-autorizado, abuso ou fraude não é limitado a uma única localidade, mas ocorre também em qualquer ponto de acesso numa rede.

Além disso, arranjos mais complexos e diversos tipos de hardware, software, organizações e pessoais são necessários para as redes de telecomunicações, criando novas áreas e oportunidades para penetração e manipulação. As redes sem fios, usando a tecnologia baseada em rádio, são mais vulneráveis à penetração porque a transmissão se dá rádio, sendo possível sua interceptação. A Internet também estabelece problemas significativos, já que foi projetada explicitamente para ser acessada com facilidade por pessoas em diferentes sistemas de computadores.

Assim, segundo [LAUDON+1999], a segurança das redes e da informação pode ser entendida como a capacidade de uma rede ou sistema de informação para resistir, com um certo nível de confiança, a eventos acidentais ou ações maliciosas que comprometem a disponibilidade, autenticidade, integridade e confiabilidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema.

2.1 Requisitos de Segurança

À medida que novas aplicações surgem, novos requisitos de segurança devem ser considerados e atendidos. O objetivo principal de um sistema de provisão de segurança é satisfazer um conjunto de requisitos impostos por qualquer sistema que pretenda transferir dados de forma segura:

- **Privacidade**: É preciso garantir que o conteúdo das transações (requerimento/resposta) seja desconhecido por terceiros, mesmo que estes tenham acesso ilícito ao canal de comunicação. Também a utilização da criptografia para proteger os pedidos dos clientes e respostas dos servidores se torna um requisito indispensável.
- **Autenticação de servidores/serviços**: um servidor deve autenticar-se perante os clientes para ter a garantia da privacidade e para que estes possam confiar nos dados e objetos enviados pelo servidor.
- **Autenticação de clientes/usuários**: Um cliente deve autenticar-se perante os servidores apresentando credenciais válidas para que o controle de acesso possa ser realizado.
- **Integridade de transações**: Deve ser garantida a integridade dos "objetos" transferidos, possibilitando a detecção imediata que dados recebidos foram corrompidos ou falsificados por pessoas indevidas.
- **Transações irreversíveis**: Deve ser garantida que uma transação ocorreu de fato entre determinadas entidades gerando um conteúdo determinado. Desta forma, impede-se que as entidades possam alterar em seu benefício o conteúdo das transações ou negar sua ocorrência. O conceito de assinatura digital deverá ser empregado sobre toda transação.
- **Certificação de objetos**: Suporte para certificação/autenticação da identidade do objeto/documento e garantia da sua integridade. Assinatura digital também é utilizada neste contexto, mas aplicada apenas sobre o objeto em si e não sobre toda a transação.

2.2 Problemas Relacionados

O uso cada vez mais freqüente das redes de computadores para a condução dos

negócios e a massificação do uso da Internet obrigou a utilização de melhores mecanismos de segurança nas transações de informações confidenciais. A questão da segurança é bem enfatizada, principalmente, quando se imagina a possibilidade das informações estarem expostas a atacantes ou intrusos da Internet que, cada vez mais possuem meios sofisticados para violar a privacidade e a segurança das comunicações.

2.2.1 Intrusos

Os intrusos, também chamados de atacantes ou usuários trapaceiros, podem se conectar de forma não autorizada em uma máquina ou, se autorizados, adquirir privilégios ou executar ações além das que lhe foram permitidas.

Podemos classificá-los como [STALLINGS2000]:

- **Masquerader**: É aquele indivíduo que não possui autorização de uso num computador, mas penetra no sistema de controle de acesso para conseguir uma conta de usuário legítimo.
- **Misfeasor**: Um usuário legítimo com acesso a dados, programas e recursos para acessos autorizados ou não, mas que abusa de seus privilégios.
- **Usuários Clandestinos**: Indivíduos que conseguem controle de supervisor do sistema e com isso, invadem a auditoria e controle de acesso.

Geralmente, o objetivo desses atacantes é ter acesso ao sistema para aumentar seu poder de acesso privilegiado.

2.2.2 Ameaças e Ataques

Numa rede ou sistema, qualquer coisa que possa afetar ou atingir o seu funcionamento, operação, disponibilidade e integridade pode ser considerada uma ameaça, e o conjunto das ações que comprometem os recursos computacionais é o ataque propriamente dito [STALLINGS1999].

Os atacantes podem apresentar comportamentos diferentes em relação às posições da origem e destino das mensagens. Na Figura 1, serão mostradas as quatro categorias de ameaças na segurança:

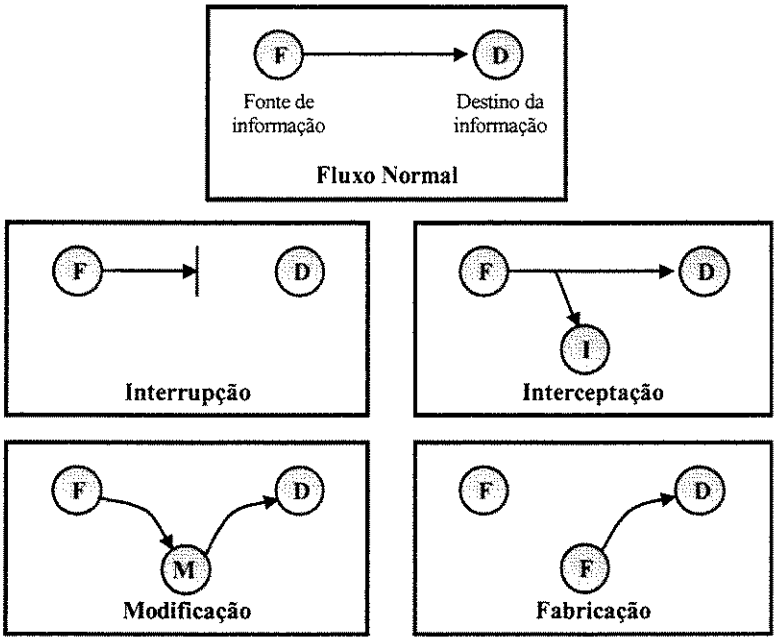


Figura 1 - Posição do atacante em relação à origem e ao destino

- **Interrupção:** O objetivo do atacante é interromper o fluxo de mensagens que partem da origem, deixando o dispositivo destino sem receber pacotes. O ataque ocorre na disposição da mensagem.
- **Interceptação:** O atacante objetiva ter conhecimento de todo o fluxo de dados que trafega pela conexão, influenciando na confiabilidade das informações.
- **Modificação:** O atacante, além de "escutar" os dados, intercepta e modifica-os, para em seguida enviá-los ao destino. Nesse caso, a integridade dos dados é desrespeitada.
- **Fabricação:** O atacante fabrica dados para enviar para o dispositivo destino, que não tem como saber quem enviou os dados. O ataque ocorre quanto à autenticidade.

A materialização de uma ameaça intencional configura um ataque. Os principais ataques que podem ocorrer num ambiente de processamento e comunicação de dados são [SOARES+1998]:

- **Personificação**: Uma entidade faz-se passar por outra, ou seja, uma entidade que possui poucos privilégios pode fingir ser outra, para obter privilégios extras.
- **Replay**: Uma mensagem, ou parte dela, é interceptada, e posteriormente transmitida para produzir um efeito não autorizado.

- **Modificação**: O conteúdo de uma mensagem é alterado, implicando em efeitos não autorizados sem que o sistema consiga detectar a alteração.
- **Recusa ou Impedimento de Serviço**: Ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades executem suas funções.
- **Ataques Internos**: Ocorrem quando usuários legítimos comportam-se de modo não autorizado ou não esperado.
- **Armadilhas (*trapdoor*)**: Ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando (emitido pela entidade que está atacando o sistema) ou a um evento, ou seqüência de eventos, predeterminados.
- **Cavalos de Tróia**: Nesse ataque, uma entidade executa funções não autorizadas, em adição às que está autorizada a executar.
- **Vírus**: Programas ou fragmentos de códigos parasitas que não funcionam de forma autônoma; requerem um hospedeiro (programa "autêntico") ao qual se anexa para infectar. São ativados pela execução dos programas infectados.

2.3 Mecanismos de Segurança

Alguns mecanismos de segurança adequados a ambientes de comunicação de dados serão discutidos a seguir. Para que um sistema possa garantir a segurança de informações, ele deve prover os seguintes requisitos básicos [SWAMINATHA+2002]:

- **Autenticação**: Os usuários, processos ou componentes de hardware são capazes de garantir a identificação das pessoas ou organizações envolvidas na comunicação.

  Quando um dispositivo *wireless* requer serviços no provedor local, ele se apresenta ao sistema como um usuário credenciado, identificando-o como um usuário autorizado.

- **Controle de Acesso e Autorização**: O processo ou componente de hardware controla os acessos a quaisquer recursos representados ou controlados por eles.

  O controle de acesso e a autorização estão fortemente relacionados com a autenticação. O controle de acesso ocorre mediante a exigência de um usuário estar autenticado para verificar se o mesmo é autorizado a utilizar o serviço.

Nos dispositivos sem fios, o controle de acesso e a autorização são conferidos através da característica de *lockout* (para que um aparelho sem fios possa ser utilizado, um código de acesso é exigido), que proporciona a proteção contra pessoas sem autorização acessando células telefônicas e assumindo a identificação de proprietário, ao usar o serviço celular.

- **Não-Repúdio**: Um usuário ou processo é identificado e responsável pelas próprias ações, de modo que isso os impeça de negar suas autorias numa data posterior.

- **Confidencialidade ou Sigilo**: Um usuário, processo ou componente de hardware tem o poder de proteger sua informação da revelação sem autorização.
  Esse mecanismo de segurança está associado, por exemplo, à proteção da informação do cartão de crédito na *Web*, às autoridades legais de e-mails e aos registros de compras on-line, por exemplo, tornando evidente que os consumidores, juntamente com as agências governamentais, se preocupam com a confidencialidade e o sigilo em redes cabeadas e sem fios.

- **Integridade**: É o princípio em que um usuário, processo, ou componente de hardware tem a capacidade de verificar a precisão do que é enviado ou entregue e que o processo ou componente de hardware não foi alterado de modo algum.
  A integridade sempre teve grande importância aos consumidores que administram transações eletronicamente, pois são manipuladas informações críticas que podem sofrer sérias conseqüências se a integridade não for mantida.

- **Auditoria**: É o princípio em que as atividades de um usuário, processo, ou componente de hardware são revisadas para assegurar que tudo o que foi executado era apropriado para a entidade em questão.
  A auditoria pode ser um processo reativo ou proativo – no reativo, os *logs* de auditoria podem ser examinados numa data posterior com uma medida *forense* para identificar a razão do problema de segurança; no proativo, os *logs* de auditoria são examinados num tempo real próximo para detectar comportamentos anormais ou impedir tentativas de evitar medidas de segurança. O processo proativo de auditoria é o preferível, mas os exames de *logs* e o monitoramento das atividades dos usuários em tempo real são recursos intensivos e que devem ser planejados cuidadosamente.

As técnicas de proteção da comunicação de dados têm evoluído muito mais no sentido do desenvolvimento de mecanismos para tornar incompreensível a um intruso os dados que são transmitidos, do que no sentido de proteger fisicamente os meios de comunicação para evitar o acesso indevido a eles.

Os modernos canais de telecomunicações envolvem meios onde a proteção física em alto grau seria impraticável; por exemplo, os longos cabos passando por vias públicas ou os enlaces de rádio que podem ser interceptados por qualquer pessoa.

2.4 I-ADD: Processo de Análise de Segurança

Num primeiro momento, a análise e o planejamento de segurança podem parecer tarefas desanimadoras. Mas, se o processo de análise de segurança for aplicado desde o início do projeto, ele pode guiar, complementar e até sustentar todo o *design* padrão do sistema. O processo de análise de segurança, chamado de I-ADD, é composto por quatro fases [SWAMINATHA+2002]:

1. **I**dentificação de objetivos e papéis.
2. **A**nálise de ataques e vulnerabilidades e geração de proteções.
3. **D**efinição da estratégia de segurança, se atentando à segurança, funcionalidade e administração.
4. ***Design*** da segurança desde o início.

Identificação

A primeira fase do processo caracteriza-se pela identificação dos blocos funcionais de alto nível do sistema. Um sistema *wireless* típico é composto por seis blocos funcionais de alto nível (conforme Figura 2). Num segundo momento, é realizada a verificação de cada um dos blocos com a intenção de identificar o recurso ou objetivos da informação dentro de cada bloco que deveria ser protegido.

Uma maneira alternativa de se proceder é identificar os papéis dos usuários nos blocos, ao invés das suas ameaças.

Para uma avaliação completa, é necessário atenção aos objetivos e papéis a serem protegidos; apenas a investigação de um ou outro pode causar vulnerabilidades ao sistema. Por exemplo, não existe nenhuma ameaça conhecida, então nenhuma proteção naquela área é necessária; reciprocamente, podem ser utilizados mecanismos excessivos para proteger um recurso que não é vulnerável a uma ameaça.

Conforme a progressão no sistema, as informações podem favorecer a identificação de papéis e objetivos adicionais que requerem proteção para blocos anteriores. Depois de completada a primeira repetição, a análise é refeita até que nenhum outro objetivo ou papel merecedor de proteção seja identificado. Assim é concluída a fase de Identificação.

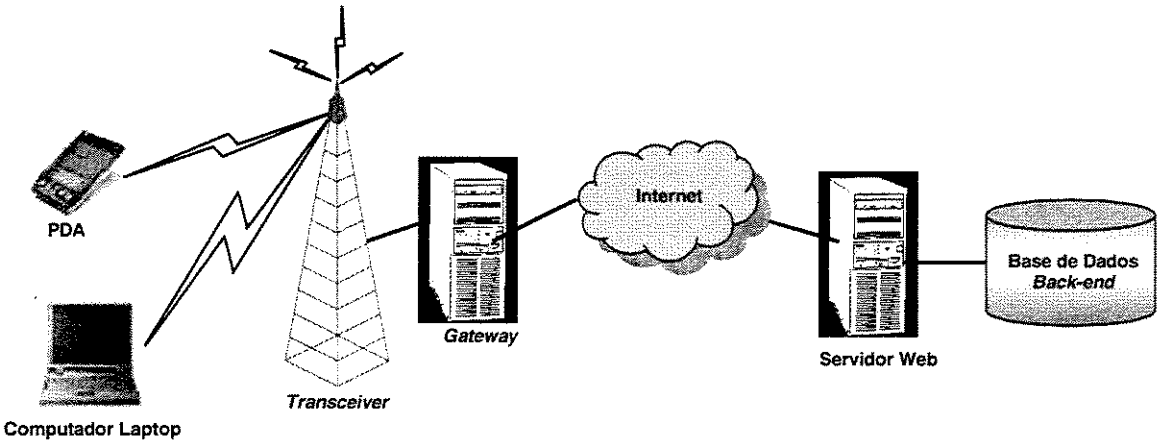


Figura 2 - Um sistema *wireless* típico

Análise

Completado o processo de identificação, é preciso analisar as vulnerabilidades e conhecer os ataques teóricos contra os objetivos, pelos vários papéis identificados. O objetivo dessa fase é compreender quais itens merecem recursos adicionais de proteção.

A fase de análise envolve as seguintes atividades:

- Estudo de ataques existentes conhecidos;
- Comparação do sistema com outros semelhantes, com o intuito de analisar como as vulnerabilidades foram resolvidas e determinar a conveniência de utilizar soluções semelhantes no caso em questão;
- Exame da segurança corrente e de documentações a respeito da tecnologia;
- Desenvolvimento e compreensão de como as soluções irão afetar outros aspectos do sistema;
- Consulta a especialistas experientes da área.

Definição

A fase de Definição define e desenvolve uma estratégia de implementação de segurança do sistema. Todos os princípios e fatores são analisados e ajustes são feitos para prover, ao sistema, o equilíbrio necessário entre os elementos definidos e guiados no

desenvolvimento do sistema.

A estratégia desenvolvida, quando feita corretamente, representa uma análise crítica dos ajustes entre a tecnologia e os objetivos do negócio e traça um caminho a ser seguido para a conclusão, com sucesso, do sistema.

Design

Com a estratégia a ser seguida, o sistema pode ser implementado de baixo para cima, incorporando características e procedimentos desenvolvidos na fase de Definição. O design deve incorporar todos os aspectos de funcionalidade apropriados, determinados nas fases anteriores. Durante esta fase, se alterações razoáveis forem necessárias, o processo pode ser reiterado para avaliar como a nova informação afetará as suposições e recomendações prévias. Quando a fase de Design estiver completada, a especificação resultante e a descrição funcional associada devem descrever o sistema completamente.

A Figura 3 mostra a representação gráfica do processo. A entrada é feita na fase de Identificação e é permitida a iteração através das quatro fases até que se consiga o *design* desejado.

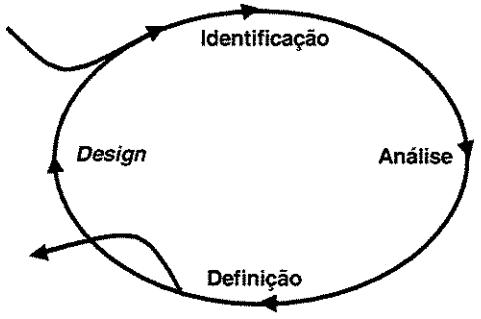


Figura 3 - O processo de análise de segurança

Repetição

A próxima etapa do processo segue um padrão recursivo no qual cada bloco é separado até o próximo nível funcional. A Figura 4 mostra um típico sistema *wireless* com os dispositivos sem fios separados até o próximo nível funcional.

Cada bloco é examinado como um sistema único, conforme a Figura 5, da mesma maneira que os blocos de alto-nível são examinados usando o processo de análise de segurança I-ADD. O processo recursivo é continuado até que os componentes de software de alto-nível forem designados ou os componentes de hardware identificados. Os resultados são retornados ao início do processo, verificando se as exigências designadas foram

incorporadas a qualquer item adicional dos níveis mais baixos.

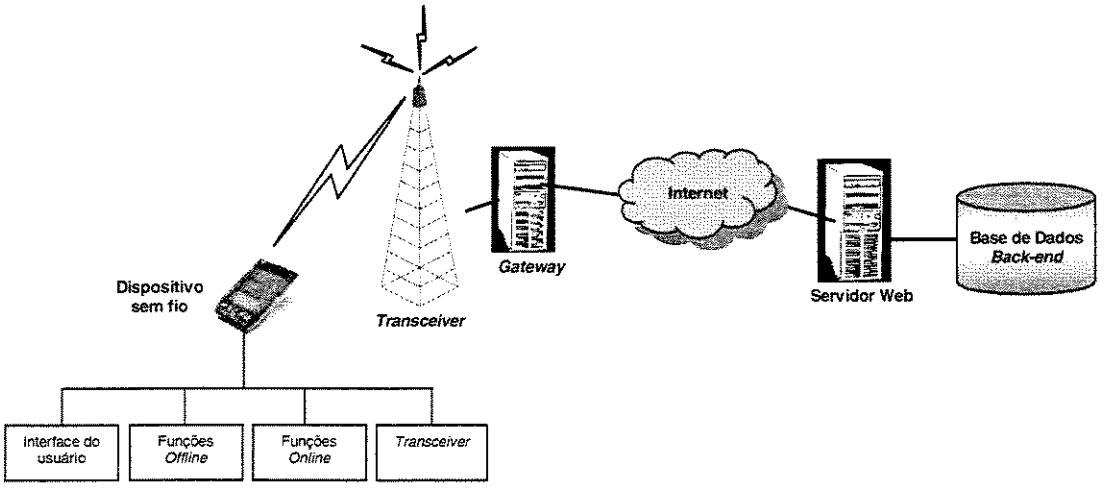


Figura 4 - Um sistema *wireless* com os dispositivos sem fios particionado para o próximo nível

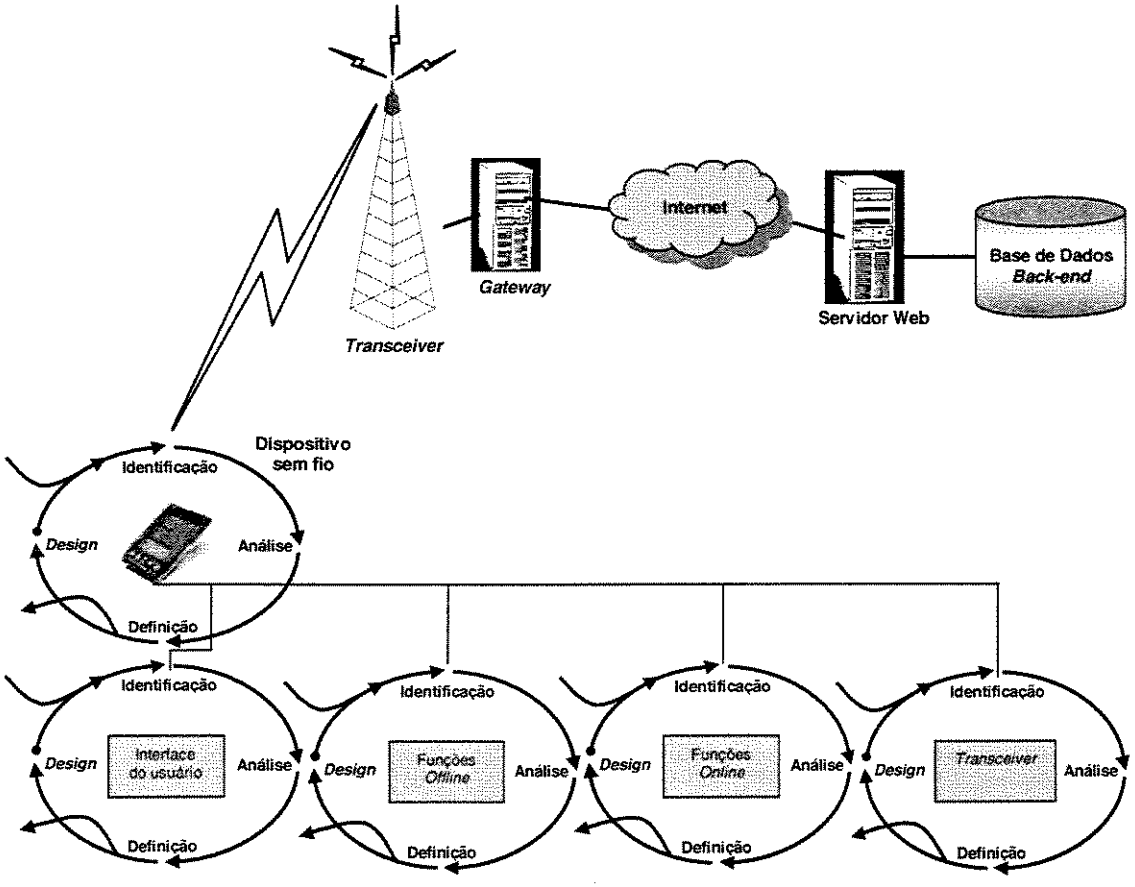


Figura 5 - Um sistema *wireless* com o processo I-ADD imposto no segundo nível do dispositivo sem fios

2.5 Sistemas de Criptografia

Os sistemas criptográficos [STALLINGS1999] englobam o conjunto de algoritmos e técnicas matemáticas sobre as quais repousam métodos e protocolos destinados ao provimento dos requisitos da segurança da informação.

A criptografia surgiu da necessidade de se enviar informações sensíveis através de meios de comunicações não confiáveis, ou seja, em meios onde não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo[1]) ou para modificá-lo (intruso ativo[2]). Tem como finalidade básica cifrar (codificar ou criptografar) uma mensagem através de um método de cifragem, que recebe como entrada a própria mensagem e uma chave de cifragem, produzindo como resultado uma mensagem cifrada. A mensagem cifrada é então armazenada em um meio qualquer ou transmitida até um receptor. Para decifrar a mensagem (decodificar ou decriptografar), utiliza-se um método de decifragem, que recebe como entrada a mensagem cifrada e uma chave de decifragem, e fornece como saída a mensagem original. A Figura 6 mostra os componentes de um sistema criptográfico.

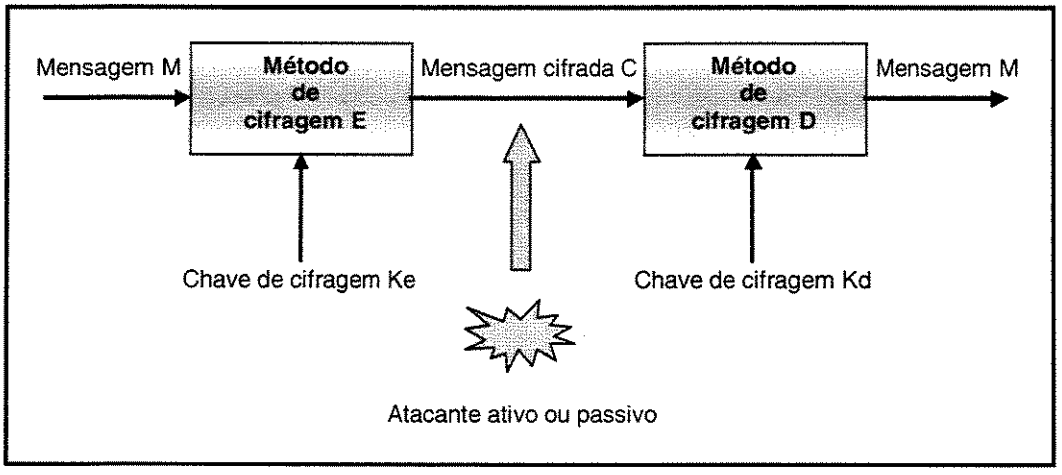


Figura 6 - Sistema de Criptografia

Os sistemas criptográficos tendem a envolver um algoritmo e um valor secreto. O valor secreto é conhecido como sendo chave. Os três tipos de funções criptográficas são criptografia de chave secreta ou simétrica, criptografia de chave pública ou assimétrica e função de *Hash*.

[1] O intruso passivo limita-se somente a escuta, cópia de informações e análise de tráfego. A ameaça ocorre apenas quanto à confiabilidade.

[2] A ação de um intruso ativo envolve a alteração da informação contida no sistema, ou modificações em seu estado ou operação.

2.5.1 Criptografia de Chave Secreta ou Simétrica

Criptografia de chave secreta utiliza apenas uma chave simples, que deverá ser mantida sob sigilo e será usada tanto para criptografar quanto para decriptografar.

O algoritmo, usando a chave, converte um documento normal em um documento cifrado. Quando o emissor cifra um documento, este só poderá ser decifrado pelo receptor que possuir o algoritmo de deciframento e a chave.

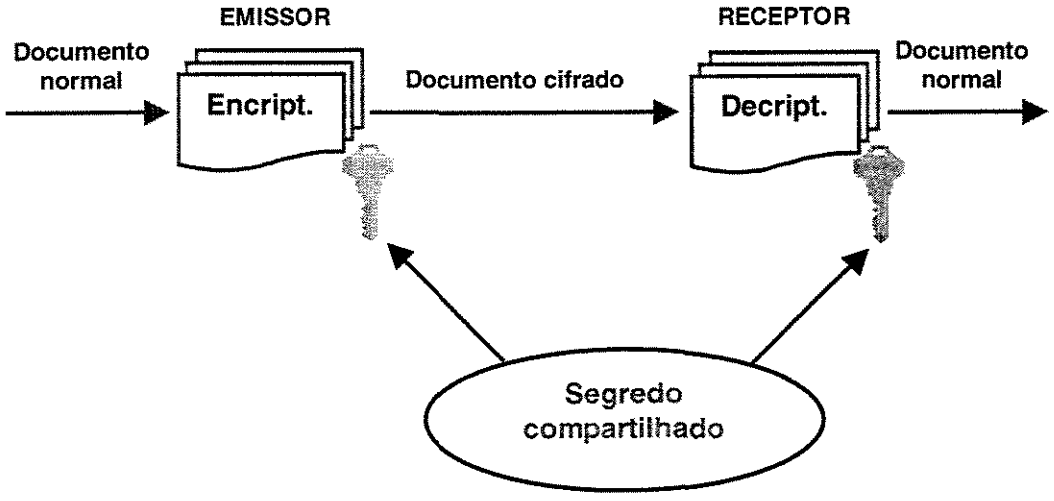


Figura 7 -Criptografia de Chave Secreta ou Simétrica

Como vantagens dos algoritmos de chave secreta, podemos citar a rapidez de execução em relação aos algoritmos de chave pública e a forte autenticação funcional que eles fornecem, pois qualquer um pode demonstrar o conhecimento do segredo sem revelá-lo. Essa funcionalidade é essencial para sistemas sem fios.

Por outro lado, como a criptografia simétrica está baseada no compartilhamento de uma mesma chave entre emissor e receptor da mensagem, o principal problema desse método é a técnica de gerenciamento da chave, pois se, por descuido ou não, uma das partes divulgar a chave, o sigilo estará comprometido.

2.5.2 Criptografia de Chave Pública ou Assimétrica

Na criptografia de chave pública são geradas duas chaves: uma pública e uma privada; o usuário deverá divulgar sua chave pública e manter em sigilo sua chave privada. As chaves são complementares no processo criptográfico, sendo que uma delas é usada

para criptografar a mensagem e a outra para decriptografar.

O emissor cifra o documento usando a sua chave privada e gera um documento criptografado. Esse documento criptografado navega pelo canal de comunicação chegando até o receptor. Este, por sua vez, pode interpretar o conteúdo, decifrando-o através da chave pública do emissor.

A autenticidade pode ser garantida; uma vez que o receptor tem a chave pública do emissor, ele pode checar a identidade do emissor, conforme visto na Figura 8.

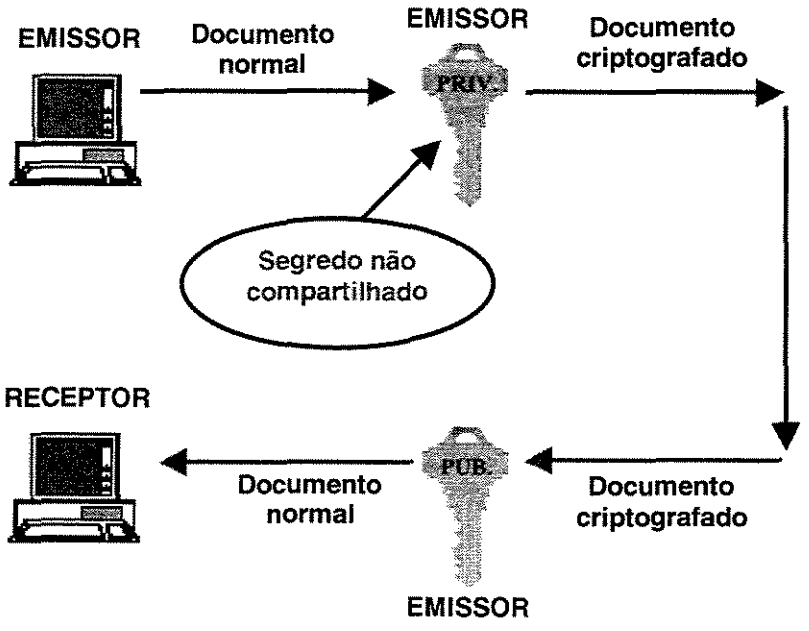


Figura 8 - Criptografia de Chave Pública garantindo a Autenticidade

Já o sigilo não pode ser verificado, pois qualquer pessoa que possuir a chave pública do emissor pode decifrar o documento. Para tanto, o emissor cifra o documento usando a chave pública do receptor e gera, assim, um documento criptografado. Esse documento cifrado trafega pelo canal de comunicação chegando até o receptor. Este, por sua vez, para poder entender o conteúdo, decifra-o usando a sua chave privada.

O sigilo está garantido porque, neste caso, a única chave capaz de decifrar o documento é a chave privada do receptor, mas a autenticidade não mais, conforme visto na Figura 9.

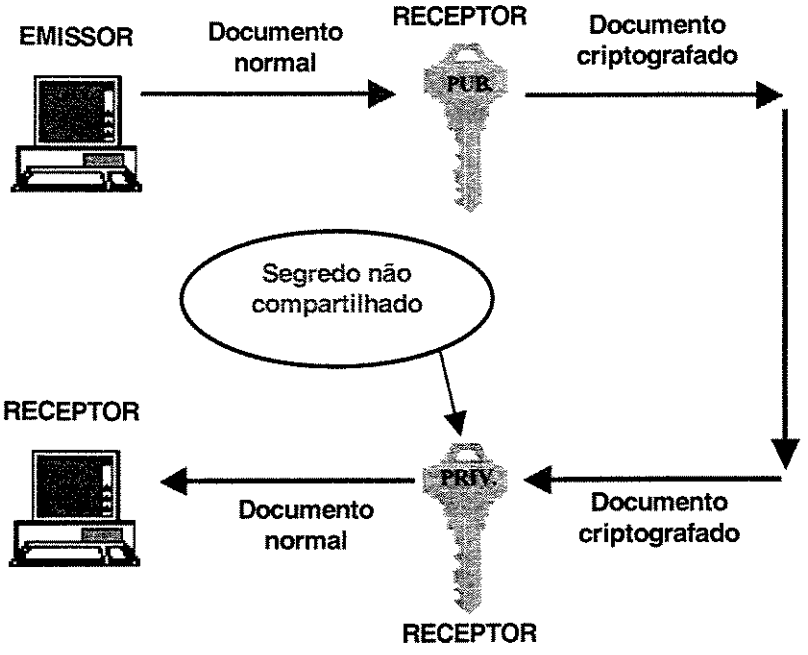


Figura 9 - Criptografia de Chave Pública garantindo o Sigilo

A criptografia de chave pública também pode ser usada para processos de autenticação, como a assinatura digital, e tem como principal vantagem a não necessidade do gerenciamento de chaves, possibilitando uma maior segurança por não compartilhar uma mesma chave criptográfica.

Apesar do alto grau de segurança da criptografia de chave pública, ela possui a grande desvantagem de ser mais lenta que a criptografia de chave secreta.

No caso das redes de comunicação, os sistemas de chave pública requerem mais recursos computacionais e transferência de um grande número de *bits*, enquanto a banda e o consumo de energia são escassos; por esse motivo, eles não são recomendados inicialmente para sistemas de comunicação sem fios.

2.5.3 Função de *Hash*

A idéia básica de uma função *hash* é truncar a informação de tal maneira que o processo não possa ser revertido. Ela recebe como entrada uma mensagem de comprimento variável e produz um bloco de comprimento fixo que representa o conteúdo da mensagem. A função deve ser tal que a mínima alteração da mensagem produz uma alteração no bloco de saída. Por outro lado, a probabilidade de se encontrar duas mensagens que produzam o

mesmo bloco de saída deve ser praticamente nula.

Como objetivos de uma função *hash* destacam-se a garantia da integridade do documento recebido e a agilidade na decifração de um documento.

Hashing pode ser usado para outras funções como uma mensagem de impressão digital, assinaturas digitais, verificação da integridade da mensagem, etc.

2.6 Aspectos desejáveis de Segurança em Comunicação Sem Fios

A estrutura e utilização de canais de comunicação compartilhados, pelos sistemas móveis, os tornam muito mais vulneráveis aos ataques. Uma infraestrutura de segurança não é só necessária como obrigatória e deve garantir aspectos como:

- **Estabelecimento da chave de sessão**: durante o processo de autenticação, uma chave de sessão, considerada um segredo comum, deve ser concordada entre o assinante e a rede servidora. Esta chave pode ser usada repetidamente, mas devido a problemas de segurança, para cada sessão, uma nova chave é requerida;
- **Sigilo das mensagens**: o ciframento da mensagem com a chave de sessão secreta estabelecida entre o assinante e a rede no processo de autenticação garantem a proteção de intrusos e da mensagem transmitida depois de uma inicialização de chamada, incluindo voz e dados;
- **Sigilo da identidade de quem está chamando**: no ambiente sem fio, um assinante tem que fornecer a sua identidade para a rede servidora para que ocorram as certificações necessárias e, a identidade do usuário e sua localização atual nunca devem ficar expostas;
- **Autenticação mútua**: as autenticações do assinante e da rede servidora devem ocorrer mutuamente, para eliminar chamadas fraudulentas;
- **Não repúdio do serviço**: mesmo não havendo associação cabeada e fixa entre o assinante e a rede, esta não deve negar os serviços prestados a ele, da mesma forma que ele nunca poderá ser cobrado injustamente, devido a erros de faturamento ou falta de segurança da rede servidora. As chamadas fraudulentas de invasores, na maioria das vezes, não podem ser distinguidas das feitas pelos assinantes.

Capítulo 3

Computação Móvel

Esta década tem presenciado um extraordinário crescimento nas áreas de comunicação celular, redes locais sem fios e serviços via satélite, o que permitirá que informações e recursos possam ser acessados em qualquer lugar e em qualquer momento. Dado o atual crescimento do segmento de computadores pessoais e PDAs (*Personal Digital Assistants*), estima-se que, em poucos anos, milhões de pessoas terão algum tipo de PDA. Independente do tipo de dispositivo portátil, a maior parte desses equipamentos deverá ter capacidade de se comunicar com a parte fixa da rede e, possivelmente, com outros computadores móveis. A esse ambiente de computação se dá o nome de computação móvel ou computação nômade [MATEUS+1998].

A computação móvel representa um novo paradigma computacional; ela surge como uma quarta revolução na computação, antecedida pelos grandes centros de processamento de dados da década de sessenta, o surgimento dos terminais nos anos setenta e das redes de computadores na década de oitenta e permite que os usuários tenham acesso aos serviços, independente de onde estão localizados, e o mais importante, de mudanças de localização, ou seja, a nomadicidade.

3.1 Características de Sistemas de Computação Móvel

Segundo [FORMAN+1994], os sistemas móveis celulares possuem algumas características e limitações que são classificadas de acordo com as seguintes macro-propriedades:

- Mobilidade dos *hosts*;
- Interface de comunicação sem fios e
- Portabilidade dos dispositivos

Mobilidade

A mobilidade pode ser caracterizada pela variação, com o tempo, do ponto de acesso à rede utilizado por um usuário. Isso ocorre devido à falta de topologia fixa de rede com

hosts móveis, o que exige que os algoritmos distribuídos tradicionais sejam reprojetados. A distribuição da carga de uma rede com elementos móveis pode ocorrer de uma maneira muito mais rápida do que em redes fixas, aumentando, com isso, o custo de localização de um elemento móvel e, conseqüentemente, o custo de cada comunicação. A manutenção das bases de informação sobre a localização de clientes móveis tem grande complexidade e a manipulação dessas informações requer estruturas de dados e algoritmos eficientes.

Numa rede móvel, o desempenho (largura de banda, latência de comunicação, etc) e a confiabilidade são afetados pela alteração na conectividade e pelo conjunto de serviços disponíveis para um elemento móvel.

Interface de Comunicação sem Fios

Para ocorrer a comunicação entre um dispositivo móvel e a Estação Rádio Base[3], uma rede sem fios é utilizada, acarretando problemas de menor largura de banda e maior latência quando comparados com a comunicação via cabos, que tem conectividade fraca e intermitente na comunicação.

A qualidade da conexão sem fios é outro fator afetado e pode variar abruptamente devido às interferências, à distância do terminal para a Estação Rádio Base (ERB) e o compartilhamento de ERBs por vários elementos móveis (a conectividade é variável). Falhas na rede também são comuns em computação móvel, já que a comunicação sem fios é muito susceptível a desconexões; quanto mais autônomo for um dispositivo móvel, maior será sua tolerância a estas desconexões freqüentes.

Os computadores móveis, ao se moverem para diferentes lugares, lidam com redes sem fios heterogêneas, obrigando-os a troca de interface devido à mobilidade.

Portabilidade dos Dispositivos

Os dispositivos (PDAs, laptops, celulares) utilizados para a comunicação sem fios por serem portáteis, precisam ser pequenos e leves, e por isso têm menos recursos: existência de pouca memória RAM, processadores mais lentos, memória não volátil pequena, interface com o usuário limitada (monitor e dispositivo de entrada de dados menores), capacidade limitada da bateria fornecedora de energia e pouca robustez, podendo ser perdidos ou roubados.

Apesar de apresentar algumas desvantagens evidenciadas acima, as redes sem fios

[3] Estação-base ou Estação de Rádio Base (ERB) é uma configuração de hardware/software que reside na torre da antena ou próxima dela. É a antena que transmite ou recebe sinais eletromagnéticos dos dispositivos numa área específica e seu poder de saída determina o alcance do sinal a ser transmitido.

também motivam o sucesso. Como exemplo podemos citar a crescente necessidade de acesso à informação (em qualquer momento e lugar); maior eficiência do trabalho, pois são permitidas a comunicação e interação em lugares variados ou em movimento; custo menor da infra-estrutura de comunicação; tendências de barateamento e miniaturização dos dispositivos móveis e ainda, a possibilidade de interligação entre prédios, ampliando a rede externa com a replicação de sinais por meio de antena.

3.2 Conceitos Básicos

A evolução da tecnologia da Informática, através dos serviços celulares, redes locais sem fios, transmissão de dados via satélite e *radio modems*, e da comunicação sem fio buscam atender muitas das necessidades do mercado. A comunicação sem fios é um suporte para a computação móvel e explora diferentes tecnologias de comunicação que serão inseridas em ambientes computacionais fixos e móveis.

Toda comunicação sem fios usa energia eletromagnética para transmitir informação; a diferença está no comprimento da onda e na freqüência.

Os sistemas móveis se baseiam, em sua grande maioria, na transmissão via rádio, ou na emissão de rádio ou sinais. Essa onda no sistema telefônico é conseqüência da fala ou dos níveis de pressão de ar produzidos, que são transformados em ondas elétricas.

As características básicas de uma onda, amplitude, freqüência e fase, podem variar em cada provedor ou serem combinadas dentro dos limites autorizados. A modulação é o processo de variação de um dos atributos citados acima, sendo os tipos mais conhecidos a modulação em amplitude (AM) e em freqüência (FM). A forma AM é a mais usada nas transmissões comerciais e é bastante sensível a ruídos; portanto, é pouco indicada para a comunicação sem fios.

Pela modulação, pode ser caracterizada a forma de apresentação da informação que se transforma em tráfego. Visando maiores velocidades de transmissão, esse tráfego deve ser cursado o mais rápido possível. Nesse sentido, surge a idéia de multiplexação, ou a agregação de várias informações para acelerar a transmissão. As técnicas de multiplexação para comunicação sem fio são a FDM (*Frequency Division Multiplexing*) e a TDM (*Time Division Multiplexing*).

Na técnica de multiplexação FDM (*Frequency Division Multiplexing*), cada sinal é transmitido em freqüências diferentes e, portanto, não se misturam. Utiliza-se a modulação para que cada sinal ocupe freqüências diferentes e a separação entre as freqüências é o suficiente para não haver interferências.

Em TDM (*Time Division Multiplexing*), múltiplos sinais podem ser transmitidos pelo mesmo meio, sendo que cada sinal ocupado durante um intervalo de tempo tem toda a banda de freqüência disponível.

Nos sistemas de comunicação existe permanente disputa de recursos em função do compartilhamento dos meios comuns. O acesso a esse compartilhamento se dá através das técnicas de multiplexação de freqüência, tempo e código, o que caracteriza um múltiplo acesso.

Os métodos ou arquiteturas de acesso de usuários existentes são o FDMA (*Frequency Division Multiple Access*), TDMA (*Time Division Multiple Access*) e CDMA (*Code Division Multiple Access*), que é o mais recente.

3.3 Métodos de Acesso para Sistemas de Comunicação Móvel

Uma das questões básicas no âmbito da Computação Sem Fios diz respeito à maneira de acesso ao meio físico de forma eficiente.

Os métodos de acesso são utilizados para permitir o compartilhamento de uma determinada faixa de rádio freqüência entre vários terminais móveis. O compartilhamento se faz necessário, pois se objetiva maximizar o número de usuários simultâneos nessa faixa de freqüência [RAPPAPORT2001], [STALLINGS2002].

3.3.1 FDMA - *Frequency Division Multiple Access*

O método de Acesso Múltiplo por Divisão em Freqüência (FDMA) é uma das primeiras técnicas de múltiplo acesso utilizada em sistemas de comunicação móvel e realiza alocação fixa do canal através da divisão da banda de freqüências em sub-bandas menores. Essas sub-bandas menores são alocadas aos usuários, normalmente, por demanda.

Em sistemas celulares, é alocado para cada célula um determinado número de canais (sub-bandas de freqüência). Os canais são atribuídos aos terminais móveis ativos cobertos pela célula, e ficam dedicados integralmente a cada terminal. O esquema de multiplexação por divisão de freqüência é ilustrado abaixo:

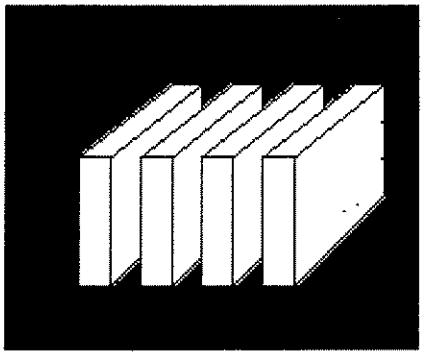


Figura 10 - Esquema de Multiplexação por Divisão de Freqüência

Apesar de sua simplicidade, FDMA apresenta uma série de desvantagens não sendo apropriado para aplicações em computação móvel; porém se aplica principalmente em sistemas analógicos que utilizam voz.

3.3.2 TDMA - *Time Division Multiple Access*

TDMA (Acesso Múltiplo por Divisão de Tempo) é uma técnica de múltiplo acesso com alocação fixa do canal, sendo bastante usada pelos sistemas móveis e sem fios. Nestes sistemas, os usuários dividem uma portadora comum para a comunicação com a estação-base, de acordo com uma política *time-shared.*

Para cada usuário transmitindo voz digitalizada ou dados, é alocado um ou mais intervalos (*slots*) de tempo dentro de um quadro, seja na direção *upstream* (do usuário para a base) como na direção *downstream* (da base para usuário).

Na direção *upstream*, cada terminal móvel ativo transmite para a base apenas no seu *slot* de tempo e na direção *downstream*, a estação-base realiza um *broadcast* para as estações móveis de acordo com uma política TDM, ilustrada na Figura 11.

O tráfego *upstream* e *downstream* é separado através do uso de diferentes portadoras FDD (*Frequency Division Duplex*) ou pela alternância no tempo TDD (*Time Division Duplex*). Enquanto que FDD requer menor largura de banda, TDD traz maior flexibilidade na alocação de banda *upstream* x *downstream.*

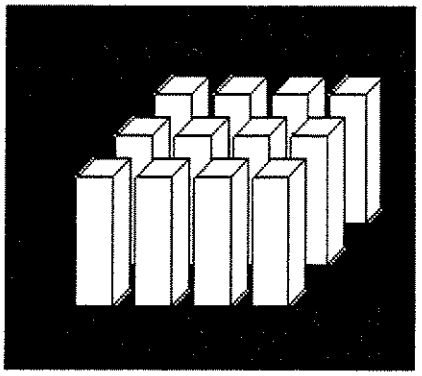


Figura 11 - Esquema de Multiplexação por Divisão de Tempo

Quando comparada com FDMA, a técnica TDMA apresenta algumas vantagens, tais como:

- maior flexibilidade na alteração do *bit rate* dos usuários, ou seja, é possível alocar mais de um *slot* de tempo para um determinado usuário dependendo da necessidade;
- um mesmo equipamento de modem e rádio, em uma dada portadora, pode ser compartilhado entre os N usuários em uma estação-base;
- a estrutura em *slots* proporciona um controle melhor;
- por ser um sistema digital, é mais seguro, podendo incorporar criptografia;
- melhor aproveitamento do espectro, já que não precisa perder banda de freqüências na separação dos canais como no FDMA.

Apesar das vantagens, o TDMA apresenta também algumas desvantagens:

- complexidade no gerenciamento e atribuição dos *slots* de tempo;
- requer equalização contra múltiplos caminhos;
- apresenta problemas de pulsação na potência do sinal (*duty cycle* de 1/N).

3.3.3 CDMA – *Code Division Multiple Access*

Nesse método de Acesso Múltiplo com Divisão por Código (CDMA) é utilizada a técnica de espalhamento espectral, onde o espectro de freqüência do sinal de informação é "espalhado" (*spread*) através de códigos não correlacionados com o sinal. Como é visto na Figura 12, todos os usuários transmitem ao mesmo tempo e utilizam a mesma faixa de freqüência.

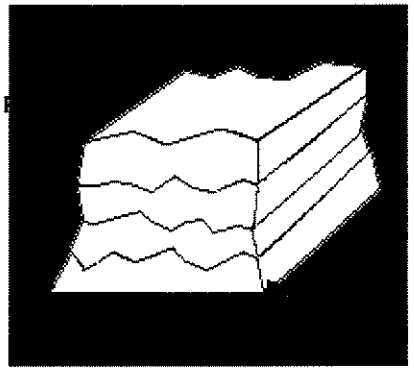


Figura 12 - Esquema de Acesso Múltiplo com Divisão por Código

Uma chamada CDMA começa com uma taxa padrão de 9600 *bits* por segundo (9,6 *kilobits* por segundo) e é "espalhada" a uma taxa de, aproximadamente, 1,23 *megabits* por segundo. Espalhar significa que os códigos digitais são aplicados a *bits* de dados associados a usuários na célula. Esses *bits* de dados são transmitidos junto com os sinais de todos os usuários restantes na célula. Quando o sinal é recebido, os códigos são removidos do sinal desejado, separando os usuários e retornando a chamada a uma taxa de 9600 bps.

Nos estágios finais de codificação da ligação de rádio com a base da estação móvel, o CDMA adiciona, ao sinal, um "código pseudo-randômico" espacial que se repete após uma quantidade de tempo finita. Estações base no sistema se distinguem umas das outras transmitindo diferentes porções de código num determinado tempo, ou seja, as estações base transmitem versões balanceadas de tempo do mesmo código pseudo-randômico. A fim de assegurar que tempos balanceados usados permaneçam únicos uns dos outros, estações CDMA têm que continuar sendo sincronizadas a uma referência de tempo comum [CDMA].

Quando implementada em sistemas de telefonia celular, a tecnologia CDMA oferece os seguintes benefícios:

- qualidade melhorada da chamada, com melhor som e mais consistente, em comparação aos sistemas analógicos;
- planejamento simplificado do sistema com o uso da mesma freqüência em cada setor de cada célula;
- privacidade realçada;
- características melhoradas de cobertura;
- tempo aumentado de conversa para portáteis;
- largura de faixa na demanda.

Para aplicações celulares, esta técnica de acesso tem sido intensamente utilizada,

sendo preferencial para muitas aplicações, como por exemplo, WLAN (IEEE 802.11), UMTS (sistema móvel europeu de terceira geração) e CDMA2000 (sistema móvel americano de terceira geração).

3.4 *Wireless*: Uma Evolução no Mundo Móvel

A computação móvel tem representado e irá representar importante papel em todo o desenvolvimento econômico global.

O "boom" da *internet* e a facilidade para se comunicar e obter informações instantâneas sobre praticamente qualquer assunto dentro de nossas casas ou escritórios gerou uma importante evolução no mundo móvel, chamada *wireless* (sem fios).

Uma conexão *wireless* é qualquer forma de conexão entre dois sistemas transmissor e receptor de dados que não requeira o uso de fios. O fato de não existirem fios ligando os dispositivos de comunicação permite que estes ofereçam mobilidade.

Embora as redes sem fios (redes *wireless*) e a computação móvel tenham forte relação, elas não são iguais: por um lado, os computadores portáteis podem ser conectados por fios e oferecer mobilidade sem o uso de uma rede sem fios (um usuário conectando um *laptop* numa tomada de telefone de um hotel, por exemplo) e por outro, alguns computadores numa rede sem fios não são portáteis, pois, quando não há cabeamento para conectar os computadores numa rede, a ligação poderá ser feita através de uma rede sem fios.

Os acessos sem fio aos serviços de telecomunicações têm demonstrado um crescimento assustador nos últimos anos. Segundo o ITU [ITU], surpreendentemente, em apenas 20 anos, os acessos sem fios irão alcançar a penetração de mercado atingida em cerca de 100 anos pelos serviços de acesso fixo convencional.

Os sistemas de comunicação móvel que utilizam o conceito de cobertura celular deverão ser a base para o que se espera dos sistemas *wireless* no futuro.

3.5 Sistemas de Redes *Wireless* e suas Tecnologias

Agrupadas sob denominação comum, temos na verdade diferentes "tipos" de redes suportadas pela tecnologia sem fios:

- **Redes WWAN (*Wireless Wide Area Network*):**

Redes celulares de Circuitos Virtuais (Telefonia Celular); redes de serviços e

comunicação pessoal ("*Personal Communication Networks*" – PCN) e redes ATM sem fio.

- **Redes WLAN (*Wireless Local Area Network*):**

Redes locais sem fio (*Wireless* LAN, IEEE 802.11); comunicação via satélite.

- **Redes WMAN (*Wireless Metropolitan Area Network*):**

Redes metropolitanas sem fio (IEEE 802.16)

- **Redes WPAN (*Wireless Personal Area Network*):**

Redes de dispositivos pessoais ("*Personal Area Networks*"); Redes de sensores.

As redes WAN sem fio, conhecidas também como WWAN (*Wireless Wide Area Network*), têm suporte na tecnologia desenvolvida inicialmente para a comunicação de voz e depois foram adaptadas para suporte a dados. Elas se baseiam, fundamentalmente, na infraestrutura da tecnologia celular existente.

As redes LAN sem fio, conhecidas também como WLAN (*Wireless Wide Area Network*), têm suporte de comunicação para interconexão de equipamentos numa área restrita, com o objetivo de viabilizar o compartilhamento dos recursos computacionais de hardware, software e informação. A organização é caracterizada por equipamentos (computadores, impressoras, terminais, servidores, etc) ligados entre si através de conexões sem fios.

As redes MAN sem fio, conhecidas também como WMAN (***Wireless Metropolitan Area Network***) oferecem uma cobertura geográfica maior que as WLANs e altas taxas de transmissão. As WMANs são padronizadas pelo IEEE 802.16 *Wireless Metropolitan Área Network Working Group*.

As redes PANs sem fio, conhecidas também como PAN (*Wireless Personal Area Network*), permitem comunicação de curta distância formando uma rede ad hoc[4] [KARAOGUZ2001] e objetivam a comunicação entre aparelhos eletrônicos e de comunicação. A tecnologia *Bluetooth* foi a primeira a surgir para este tipo de atendimento, com baixa potência de consumo, tamanho reduzido e baixo custo.

[4] A expressão rede ad hoc significa a habilidade que a rede tem de auto-configuração, assumindo automaticamente a condição de mestre/escravo e a facilidade com que os dispositivos podem fazer ou desfazer parte desta rede.

Capítulo 4

Redes *Wireless* WAN

O acesso às redes WAN sem fios é baseado nos sistemas de tecnologia celular existentes.

Nesse tipo de rede, é mais evidente a localização de um elemento móvel e, conseqüentemente, seu ponto de acesso à rede fixa, à medida que o usuário se move pela rede. As WWAN permitem que os dispositivos se conectem, através de protocolos e tecnologia sem fios, a Internet, intranet ou ao serviço de *email*. Dependendo da entidade conectada, as WANs sem fios são administradas pelas operadoras de serviços celulares, provedores de aplicação ou corporações.

As WWAN estão se expandindo para proporcionar, cada vez mais, cobertura sem fios a outras áreas do mundo.

4.1 Evolução dos Sistemas Celulares

A telefonia móvel tornou-se popular com a introdução dos telefones celulares. Essa invenção despertou excessivo interesse e viu-se em poucos anos uma verdadeira explosão mundial no seu uso.

O nome celular é decorrente do fato de a rede de comunicação ser composta de uma rede de células, com transceptores de rádio, chamada estação-base, no centro de cada célula. A célula é a área de cobertura de uma única estação-base. À medida que um telefone móvel se desloca de uma rede para outra, ele tem acesso por intermédio da estação-base da célula em que se encontra naquele momento.

A mobilidade ocorre devido ao fato do usuário poder se deslocar de um local a outro, e conseqüentemente, de uma célula para outra. O processo de comutação do celular de uma célula para outra, enquanto a ligação está em andamento, é chamado de *handover* [TAURION2002].

A indústria classifica os sistemas de telefonia celular em gerações, conforme serão descritas a seguir [AGRAWAL+1999], [DORNAN2002]:

- **1G (1ª Geração de Celulares)**: Os telefones de primeira geração são analógicos, ou seja, enviam informações como uma forma de onda continuamente variável. São usados apenas para voz e sua qualidade de recepção é variável devido às interferências. Também são poucos seguros, pois com um simples sincronizador de rádio pode-se interceptar ligações e cloná-los. São baseados no padrão AMPS (*Advanced Mobile Phone System*) que implementam o CDPD (*Cellular Digital Packet Data*) sobre a rede, utilizando um único canal em cada célula para os dados, com capacidades máximas de 19,2 kbps de entrada e 9,6 kbps de saída.
- **2G (2ª Geração de Celulares)**: Os telefones de segunda geração convertem toda a fala em código digital, o que resulta em um sinal mais nítido que pode ser criptografado visando a segurança. Possuem recursos de mensagens, correio de voz e identificador de chamadas. Utilizam as tecnologias CDMA (*Code Division Multiple Access*), TDMA (*Time Division Multiple Access*) e o GSM (*Global System for Mobile Communications*), sendo esta última a mais popular e utilizada mundialmente.
- **2,5G (Geração de transição)**: Essa geração representa uma etapa intermediária antes da 3G. Aqui, as velocidades são superiores à 2G, devido a utilização de tecnologias de pacotes que permitem acesso à Internet mais flexível e eficiente. O termo 2,5G se aplica às tecnologias HSCSD (*High-Speed Circuit-Switched Data*), GPRS (*General Packet Radio Service*) e EDGE (*Enhanced Data Rates for Global Evolution*).
- **3G (3ª Geração de Celulares)**: Os sistemas de terceira geração ainda estão nos seus primórdios. Eles proporcionarão serviços avançados como transferência de dados com alta velocidade e videoconferências. As tecnologias da 3ª geração de celulares incluem o UMTS (*Universal Mobile Telecommunications System*), o WCDMA (*Wideband CDMA*) e o CDMA2000.
- **4G (4ª Geração de Celulares)**: As redes de quarta geração ainda se encontram nos laboratórios e planeja-se implementá-las a partir de 2010. Essas redes fornecerão transparências de dados de até 100 Mbps, suficientes para a telepresença.[5]

Hoje em dia, a maioria dos sistemas de telefonia existentes pertence à segunda geração (2G). As gerações 2,5G e 3G trarão benefícios relativos à Internet móvel, com

[5] Telepresença é um tipo de realidade virtual, definida como uma estimulação completa de todos os sentidos necessários para proporcionar a ilusão de ser uma pessoa de verdade – uma ilusão que não se consegue diferenciar do objeto real.

velocidades muito maiores e a adoção da tecnologia de pacotes, que permitirá acessos à Internet com custos muito mais baratos.

As tecnologias 3G estão em experiência, mas não se sabe se elas realmente acontecerão; as companhias européias de telefonia celular fizeram investimentos altíssimos sem a garantia de retorno e ainda enfrentam o problema da diminuição da demanda de celulares na Europa.

No Brasil e na América Latina, apesar do uso limitado do SMS (*Short Message Service*) e do WAP (*Wireless Application Protocol*), as operadoras terão que decidir sobre as novas redes e, conseqüentemente, apostar no futuro da Internet móvel. Os investimentos são pesados e a migração para uma nova geração é gradual, tendo-se que conviver com diferentes configurações de redes durante muito tempo.

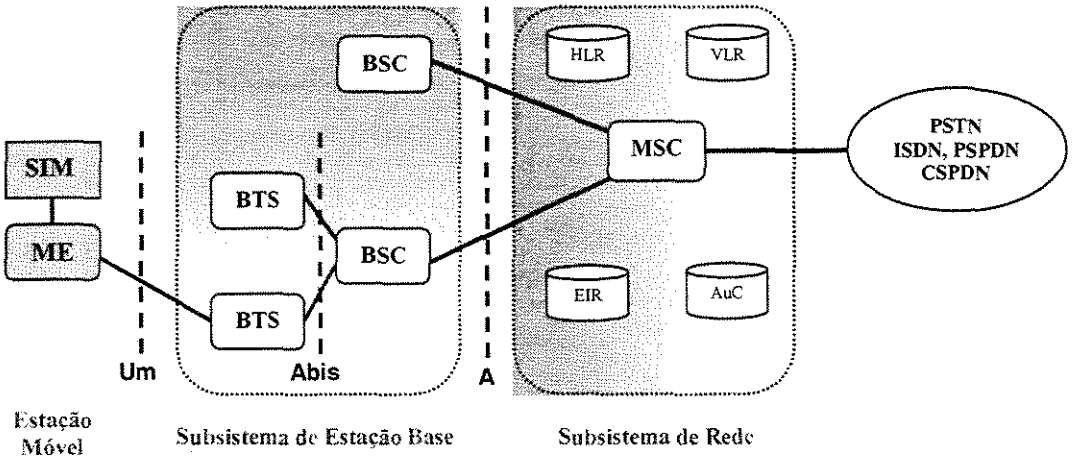
4.2 A Tecnologia GSM (*Global System for Mobile Communications*)

A tecnologia GSM (*Global System for Mobile Communications*) foi desenvolvida na Europa pelo ETSI (*European Telecommunications Standards Institute*) para fornecer um único padrão de telefonia celular digital para a comunidade européia e está se tornando um sistema global para comunicações móveis. Sua popularidade se deve à voz de qualidade relativamente alta e a facilidade de atualização para velocidades de dados superiores [WATKINS2000].

O GSM é um sistema de segunda geração baseado no TDMA (*Time Division Multiple Access*) e possui duas bandas de freqüência definidas para ele, uma de 890 até 915 MHz, para a transmissão da unidade móvel e outra de 935 até 960 MHz, para a transmissão da estação base.

4.2.1 Arquitetura das Redes GSM

O GSM possui uma arquitetura semelhante aos demais sistemas de telefonia celular. Uma rede GSM é composta por várias entidades com funções e interfaces específicas, sendo composta por três elementos básicos: estação móvel, subsistema de estação base e subsistema de rede [SCOURIAS].



SIM – Subscriber Identify Module
ME – Mobile Equipment
BTS – Base Transceiver Station
BSC – Base Station Controller
HLR – Home Location Register
VLR – Visitor Location Register
MSC – Mobile services Switching Center
EIR – Equipment Identify Register
AuC – Authentication Center

Figura 13 - Estrutura de uma Rede GSM

Estação Móvel ou MS (*Mobile Station*)

A estação móvel é composta por um equipamento móvel (terminal) e um cartão inteligente designado de SIM (*Subscriber Identify Module*). O cartão providencia mobilidade pessoal, de tal forma que o assinante consegue ter acesso aos serviços subscritos independentemente do terminal utilizado, isto é, ao inserir o cartão SIM num terminal diferente, o assinante pode usufruir os serviços a partir desse terminal. O cartão SIM tem uma identificação única mundial (IMSI), assim como o terminal (IMEI). Estes códigos são independentes, permitindo uma maior mobilidade e uma segurança pessoal contra o uso não autorizado.

Subsistema de Estação Base ou BSS (*Base Station Subsystem*)

O subsistema de estação base se encarrega do controle de ligação rádio com a estação móvel. É dividido em duas partes: a estação rádio base de transmissão (BTS – *Base Transceiver Station*) e a estação rádio base de controle (BSC – *Base Station Controller*). A BTS engloba a antena e o equipamento de rádio ao qual a estação móvel (MS) se liga; cada BTS forma uma célula de rede. Numa grande área urbana, a quantidade de BTS's deverá existir em maior número. A BSC gerencia os recursos para uma ou mais BTS's, tais como, configuração dos canais rádio, saltos de freqüência e transição entre células (*hand-over*). A BSC realiza a conexão entre as estações móveis (celulares) e o centro de comutação móvel

(MSC).

Subsistema de Rede ou NSS (*Network Subsystem*)

O seu principal componente é o MSC (*Mobile services Switching Center*), que se encarrega de fazer a comutação de chamadas entre estações móveis ou entre uma estação móvel e um terminal fixo. É ele que providencia toda a funcionalidade necessária para o tratamento de um assinante móvel, realizando o registro, autenticação, atualização da localização, transição entre células (*hand-off*) e gerenciando a mobilidade. Seu principal papel, portanto, é gerenciar as comunicações entre os usuários GSM com usuários de outras redes de comunicações.

O subsistema de rede é formado por cinco entidades funcionais: MSC, HLR, VLR, EIR, AuC. O HLR, o VLR e o MSC, em conjunto, providenciam as capacidades de mobilidade do GSM.

O HLR (*Home Location Register*) contém toda a informação administrativa de todo o assinante registrado na correspondente rede de GSM, juntamente com a localização da estação móvel. A localização da estação móvel está geralmente na forma do endereçamento do VLR (*Visitor Location Register*). As informações fornecidas pelo VLR são necessárias para controlar a chamada e providenciar os serviços de cada assinante, situada dentro de uma determinada área de controle. Outros dois registros são usados para segurança e autenticação. O EIR (*Equipment Switching Center*) é uma base de dados que contém listagens de todos os equipamentos móveis válidos na rede, onde todas as estações móveis são identificadas pelo IMEI (*International Mobile Equipment Identify Code*). A partir de um IMEI, obtém-se os seguintes status [LORD2003]:

- ***Whitelisted* (Tudo OK):** O aparelho pode conectar-se à rede.
- ***Greylisted* (Atenção):** Sob observação: normalmente este status é dado a celulares sob suspeita de clonagem ou falta de pagamento.
- ***Blacklisted* (Não Aprovado):** O terminal foi roubado, ou algum outro problema impede o celular de conectar-se à rede.

Um IMEI é considerado como inválido se declarado como roubado ou incompatível com a rede. O AuC (*Authentication* Center) é uma base de dados protegida que guarda uma cópia do código de cada SIM, usado para autenticar e criptografar através do canal de rádio.

As freqüências disponíveis são divididas em duas bandas. Cada banda é dividida em *slots* de 200 kHz, denominados ARFCN (Número Absoluto de Canal de Radiofreqüência).

Além de dividir a freqüência em fatias, o tempo também é dividido. Cada ARFCN é compartilhado por oito unidades móveis, sendo usado por uma delas por vez. Cada unidade móvel usa o ARFCN por um TS (*timeslot*) e, em seguida, aguarda a sua vez de usá-lo novamente. As unidades móveis usam o ARFCN uma vez por quadro do TDMA.

4.2.2 Benefícios das Redes GSM

O padrão GSM para a comunicação de celulares móveis digitais apresenta alguns benefícios não evidenciados nos antigos sistemas de celulares analógicos, tais como:

Mobilidade Total: os usuários podem se comunicar em qualquer lugar e serem chamados em alguma área servida pela rede celular GSM, usando o mesmo número de telefone atribuído, até mesmo fora de sua localização. Não é necessário informar o local da pessoa chamada, pois a rede GSM se encarrega dessa tarefa. Essa característica de mobilidade é preferida por pessoas de negócios que constantemente necessitam estar em contato com a sede da empresa, por exemplo.

Alta Capacidade e Ótima Distribuição do Espectro: as redes celulares analógicas anteriores tiveram que combater problemas de capacidade, particularmente em áreas metropolitanas. Pela utilização mais eficiente da freqüência fixada de banda larga e do tamanho menor das células, o sistema GSM é capaz de atender um número maior de usuários. O ótimo uso do espectro disponível é alcançado através da aplicação do Acesso Múltiplo por Divisão de Freqüência (FDMA), do Acesso Múltiplo por Divisão de Tempo (TDMA), das eficientes taxas média e alta de codificação de fala e do esquema de modulação GMSK (*Gaussian Minimum Shift Keying*).

Segurança: Os métodos de segurança padronizados para os sistemas GSM compõem hoje o padrão de telecomunicação celular mais seguro disponível. Embora a confidencialidade da chamada e o anonimato do usuário GSM somente são garantidos no canal de rádio, este é o principal passo para a segurança fim-a-fim alcançada. O anonimato do usuário é assegurado pelo uso de números identificadores temporários, e a confidencialidade de sua comunicação no link de rádio é executada pela aplicação de algoritmos criptográficos e saltos de freqüência que pudessem ser realizados em sistemas digitais.

Serviços: Os serviços disponíveis aos usuários GSM incluem comunicação de voz,

fax, *mail* de voz, transmissão de mensagens curtas, transmissão de dados e serviços suplementares com chamadas despachadas.

4.2.3 Segurança em WAN's Sem Fio GSM

Um dos principais recursos do sistema GSM é a segurança. Foi a primeira arquitetura de rede celular móvel a fornecer os serviços de segurança, como autenticação do usuário, sigilo do tráfego e distribuição das chaves.

Os objetivos para a segurança dos sistemas GSM são [MARGRAVE]:

Anonimato: garantir que não é fácil identificar o utilizador.

Confidencialidade dos Dados: garantir que os dados não são compreendidos por terceiros.

Confidencialidade da Sinalização: garantir a confidencialidade da sinalização, como por exemplo, o número de telefone.

Autenticação: garantir que quem está utilizando o sistema é a entidade correta.

A estação base faz o controle se a cifragem está ativada ou desativada. A criptografia dos dados ocorre após os dados terem sido intercalados e arranjados em oito blocos de dados (antes que os *bursts* finais sejam montados). Os algoritmos de criptografia são controlados com bastante rigor, e a segurança destes algoritmos é aumentada pelo fato do sistema trocar a chave criptográfica a cada chamada (mesmo se um algoritmo for decifrado em uma chamada, a criptografia usada na próxima chamada será diferente).

A segurança em ambientes GSM envolve aspectos de autenticação e confidencialidade da identidade do usuário e localização do assinante. O usuário é unicamente identificado pelo IMSI (*International Mobile Subscriber Identify*), e essa informação, juntamente com a chave de autenticação individual do assinante (Ki), constituem credenciais de identificação sensíveis. O modelo de autenticação GSM e os esquemas de encriptação nunca permitem que informações sensíveis sejam transmitidas no canal de rádio; um mecanismo de desafio-resposta é usado para realizar a autenticação. As conversações atuais são codificadas usando uma chave cifrada (Kc) gerada temporária e randomicamente e a Estação Móvel (MS) se identifica através do Identificador de Usuário Móvel Temporário (TMSI – *Temporary Mobile Subscriber Identify*), que é emitido pela rede e pode ser modificado periodicamente, para segurança adicional.

Os mecanismos de segurança em GSM são implementados em três diferentes

elementos: no Módulo Identificador de Usuário (SIM), na Estação Móvel (MS) e no subsistema de rede NSS.

O SIM é um cartão inteligente (*smartcard*) e possui o IMSI, a chave de autenticação individual do assinante (Ki), o algoritmo gerador de chave cifrada (A8), o algoritmo de autenticação (A3), um Número de Identificação Pessoal (PIN – *Personal Identification Number*) e o algoritmo de cifragem (A5). Toda vez que o usuário quiser utilizar uma MS, um SIM deve ser inserido, a fim de fornecer mobilidade pessoal.

O Centro de Autenticação (AUC) consiste numa base de dados de informações de identificação e autenticação para os usuários e a informação é formada pelo IMSI, TMSI, por um Identificador de Localização de Área (LAI – *Location Area Identity*) e pela chave de autenticação individual do assinante (Ki), para cada usuário.

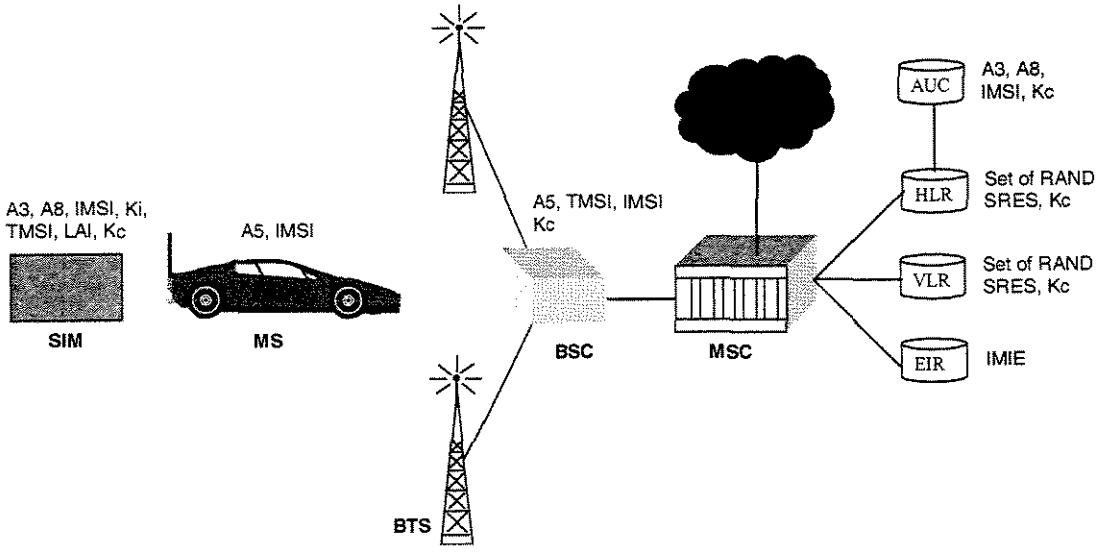


Figura 14 - Distribuição dos Parâmetros de Segurança na Rede GSM

4.2.3.1 Os Algoritmos Criptográficos A3, A5 e A8

O GSM utiliza três algoritmos criptográficos especiais: A8, A5 e A3.

O A8 é um algoritmo que utiliza uma função unidirecional usada para gerar chaves de sessão (Kc). O algoritmo A8 recebe o par (K_i, RAND) e gera a chave de sessão K_c, conforme a Figura 15.

Na prática, os operadores GSM utilizam o algoritmo COM128 para os algoritmos A3 e A8.

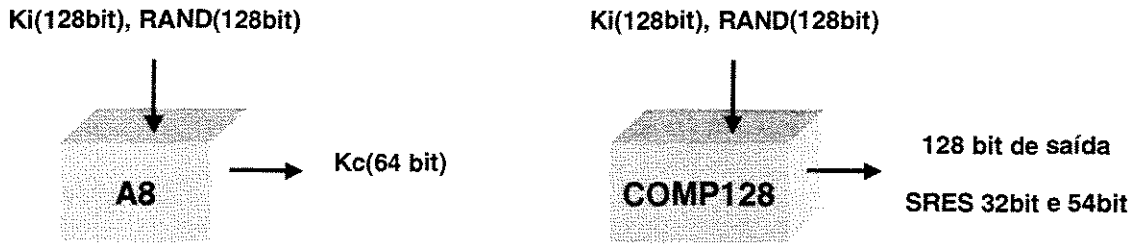


Figura 15 - O Algoritmo A8

Os últimos 54 *bits* do *output* do COMP128 são usados para a Kc. A esses 54 *bits* acrescenta-se 10 *bits* com valor 0 (zero) para completar os 64 *bits* necessários para formar a chave de sessão Kc, o que reduz drasticamente o espaço de chaves possíveis.

O A5 é um algoritmo de ciframento/deciframento de chave secreta. Ele recebe o par (K_c, *Frame Number*) e gera uma *KeyStream* de 228 *bits*; para cada frame é incrementado o *Frame Number* e gerada uma nova *KeyStream*. A *KeyStream* resultante é o XOR dos três *bits* de *output*.

Desse modo, a *KeyStream* gerada na MS é exatamente igual à *KeyStream* gerada na BTS e que são sincronizadas uma com a outra.

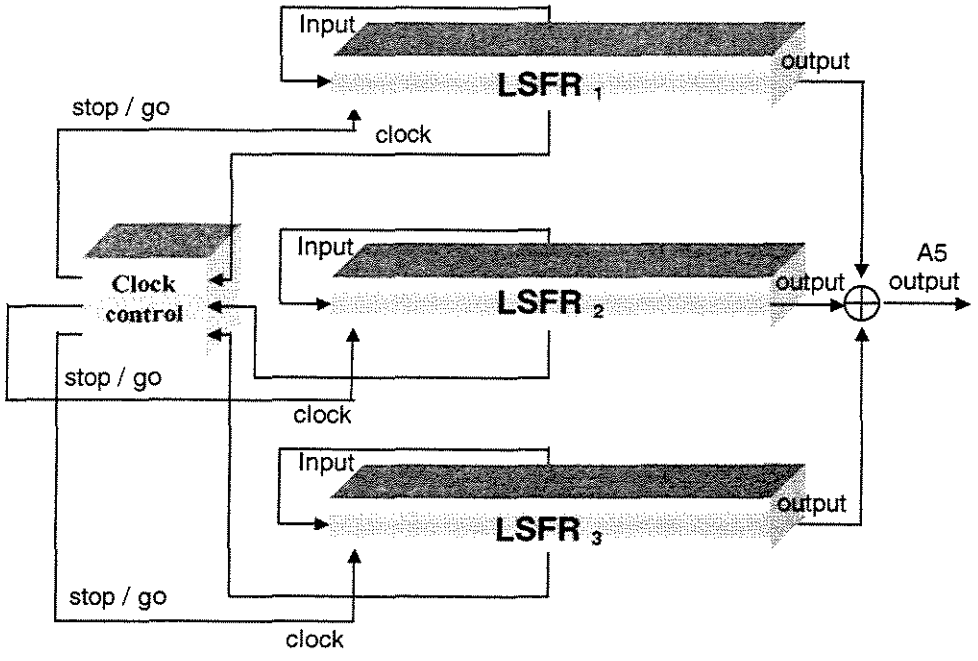


Figura 16 - O Algoritmo A5

Os 114 *bits* iniciais são usados para o envio de dados e os 114 *bits* finais são usados

na recepção.

O A3 é um algoritmo que utiliza uma outra função unidirecional, usada pelo assinante, para responder ao desafio feito pelo VLR. O algoritmo A3 recebe o par (K_i , RAND) e gera o SRES.

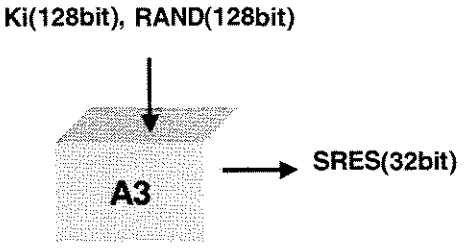


Figura 17 - Algoritmo Criptográfico A3

O algoritmo COMP128 também é usado para o algoritmo A3; ele gera um *output* de 128 *bits* a partir do par (K_i , RAND) e os primeiros 32 *bits* desse *output* são o SRES.

4.2.3.2 Autenticação Da Estação Móvel

A autenticação da identidade do assinante, numa rede GSM, é realizada através de um mecanismo de desafio-resposta. Um número randômico de 128 *bits* (RAND) é enviado à estação móvel (MS) que, com base na encriptação do número randômico (RAND) pelo algoritmo de autenticação (A3) usando a chave de autenticação individual do assinante (Ki), calcula o número SRES (*Signed Response*) de 32 *bits*. Ao receber o SRES, a rede GSM repete os cálculos para verificar a identidade do assinante. Se o SRES recebido for igual ao valor calculado, o processo de autenticação teve sucesso e a estação móvel continua em funcionamento; se os valores não correspondem, a conexão é terminada e uma falha de autenticação é indicada à estação móvel. A Figura 18 ilustra o mecanismo de autenticação.

O cálculo da resposta assinada é processado dentro do SIM, fornecendo maior segurança, pois informações confidenciais do assinante, como o IMSI ou a chave de autenticação individual do assinante (Ki), nunca são liberadas do SIM durante o processo de autenticação.

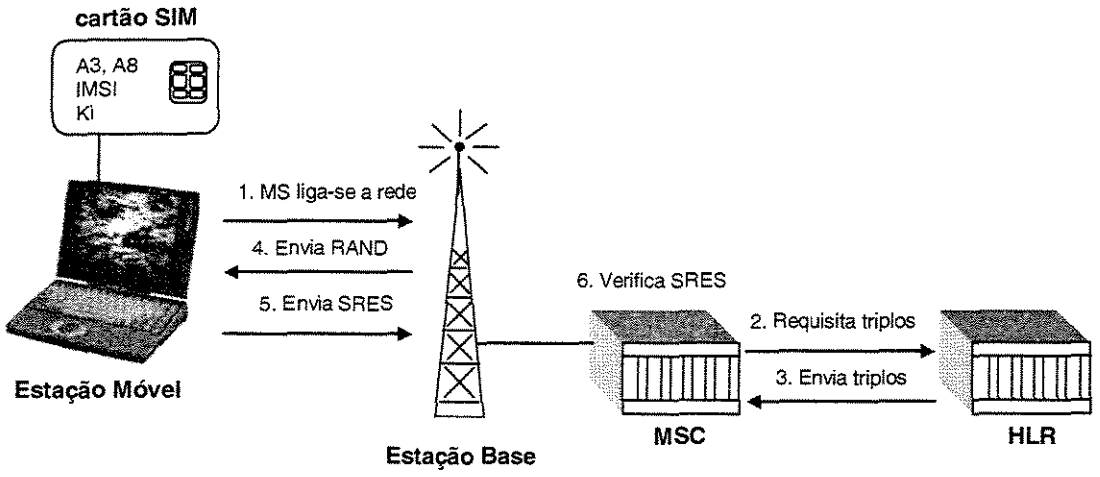


Figura 18 - Mecanismo de Autenticação

4.2.3.3 Confidencialidade Dos Dados

O SIM utiliza o algoritmo gerador de chave cifrada (A8) para produzir a chave criptográfica (Kc) de 64 *bits*. O algoritmo A8, para computar a chave Kc, recebe como entrada o mesmo número randômico (RAND) usado no processo de autenticação e a chave de autenticação individual do assinante (Ki), conforme a Figura 19.

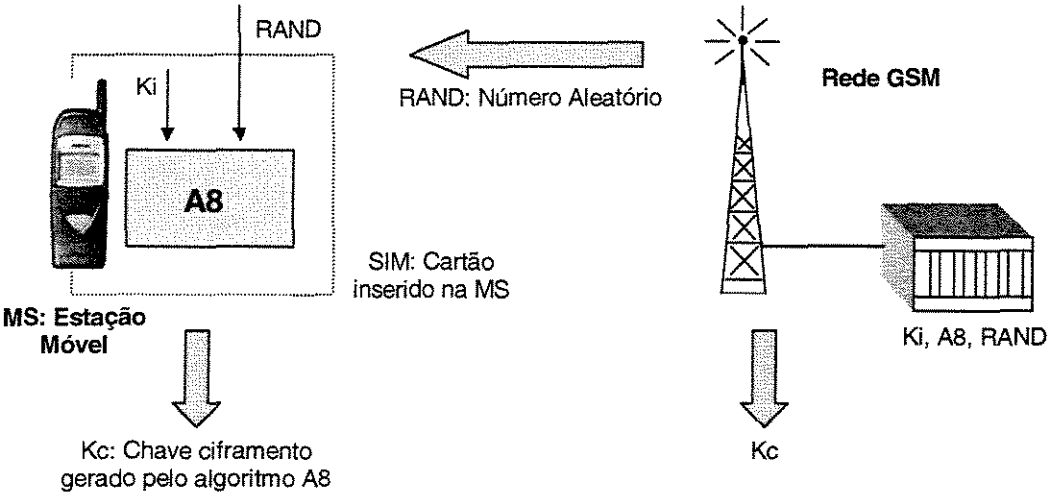


Figura 19 - Cálculo da Chave Criptográfica Kc

A chave de sessão Kc é usada para cifrar e decifrar os dados entre a estação móvel

(MS) e a estação base (BS – *Base Station*). A chave criptográfica é trocada em intervalos regulares de tempo, por desígnio da rede ou considerações de segurança, fornecendo um nível adicional de segurança e tornando o sistema mais resistente a ataques.

De uma maneira similar ao processo de autenticação, a computação da chave criptográfica Kc é feita internamente no SIM; que nunca revela essa informação sigilosa.

A codificação da voz e a comunicação dos dados entre a MS e a rede são realizadas pelo uso do algoritmo de criptografia A5. Como é visto na Figura 20, a comunicação cifrada é inicializada por um pedido de modo cifrado à rede GSM e após o recebimento, a estação móvel começa a criptografar e a decriptografar os dados usando o algoritmo A5 e a chave cifrada Kc.

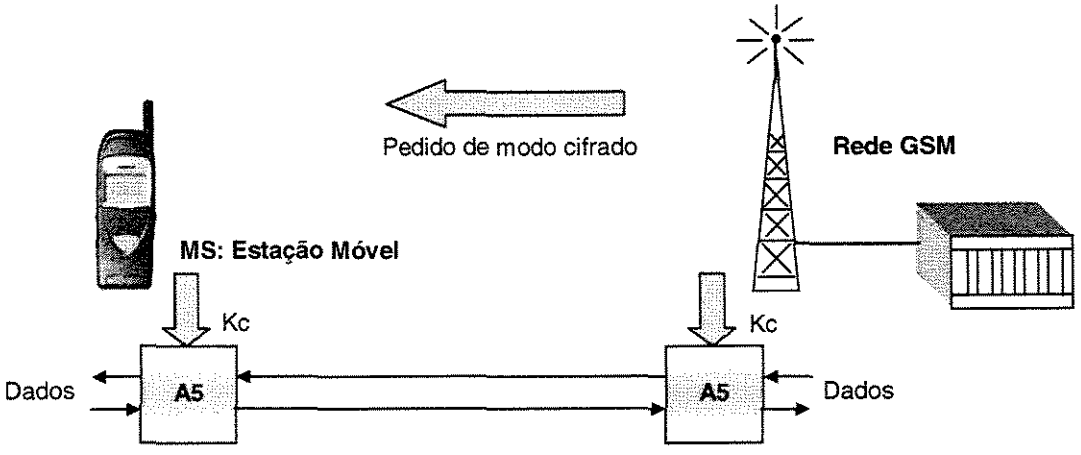


Figura 20 - Início do Modo de Comunicação Cifrada

4.2.3.4 Confidencialidade Da Identidade do Assinante

A confidencialidade da identidade do usuário é mantida pelo uso do parâmetro de Identificação Temporária do Assinante Móvel TMSI. O TMSI é enviado à estação móvel depois da conclusão dos procedimentos de autenticação e encriptação. A estação móvel confirma a recepção do TMSI e este se torna válido somente na área de localização em que está sendo usado.

Para comunicações fora da área de localização, é necessário também o Identificador de Localização de Área LAI em adição ao TMSI. O processo de alocação/relocação do TMSI é mostrado na Figura 20.

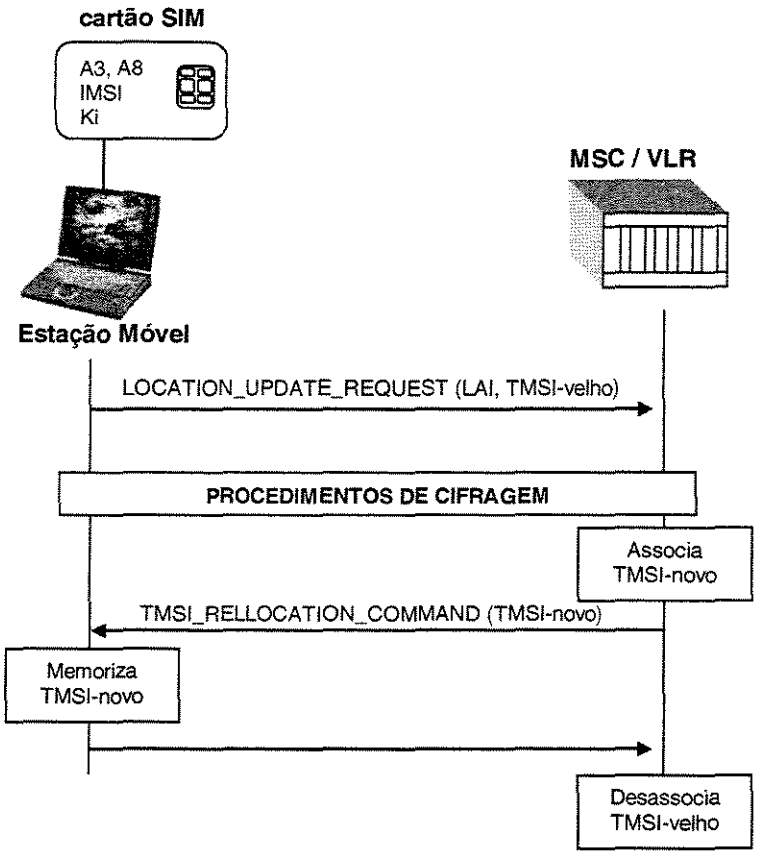


Figura 21 - TMSI Alocação/Relocação

4.2.4 Problemas de Segurança com o Padrão GSM

O sistema GSM apresenta inúmeras vantagens técnicas aos usuários que utilizarem a transmissão de dados sobre esta banda de alta velocidade de conexão e confiabilidade garantida. É verdade que a tecnologia acopla novos mecanismos de segurança, mas convém ficar alerta à disponibilidade dos mecanismos que permitem reeditar antigos problemas de segurança.

Ainda é possível clonar um SIM GSM contendo as informações do assinante, com base na engenharia reversa de seu algoritmo (COMP128), derivado de outro algoritmo chamado A5/1. Enviando um número grande de desafios para o módulo de autenticação, é fácil deduzir, em poucas horas, o valor de Ki.

Outros aspectos de segurança são descritos a seguir:

- As freqüentes interferências no sinal e outras falhas no sistema provocam a perda da sincronização do TMSI, quando o assinante é forçado a enviar o TMSI para a estação móvel, tornando exposta sua verdadeira identidade;
- A chave de sessão Kc utiliza somente 54 *bits* do total de 64 *bits*. Os 10 *bits* restantes são substituídos por zeros, o que torna a chave cifrada propositalmente mais fraca. Se essa chave Kc estiver comprometida e mandar de volta o RAND e o SRES que já foram transmitidos, um intruso poderá representar um legítimo VLR, estabelecer uma falsa conexão com o assinante e capturar informações sigilosas antes de ser detectado;
- O armazenamento do RAND, SRES e Kc no VLR têm a vantagem de acelerar o processo de autenticação, mas a desvantagem de aumentar a exposição das informações. Os intrusos podem roubá-las fisicamente para fazer chamadas fraudulentas ou divulgar a conversa do assinante;
- O ciframento é aplicado somente no canal de rádio, e não dentro de "toda a rede GSM";
- O esquema projetado é o convencional de segurança centralizada, o que exige tempo e custo adicionais, e não pode ser satisfatório, eficiente ou lógico para o futuro crescimento dos serviços de comunicações móveis.

4.2.5 Exemplos de Ataques à Tecnologia GSM

O GSM, apesar de ser a tecnologia de comunicação móvel mais utilizada na atualidade, apresenta vulnerabilidades de segurança que podem ser comprovadas através de casos verídicos.

O principal algoritmo de encriptação usado para autenticar clientes numa rede GSM, conhecido como COMP128, foi quebrado em apenas um dia por David Wagner e Ian Goldberg [BRICENO+01]. Depois de verificar várias falhas no algoritmo, os pesquisadores conseguiram também clonar aparelhos GSM, explorando a fraqueza do A3 implementado no COMP128, uma implementação conjunta das funcionalidades de A3 e A8 inicialmente secreta mas revelada por engenharia reversa [BRICENO+01], [BRICENO+02].

Para evitar espionagens casuais, o mecanismo criptográfico A5 é usado para encriptar a comunicação entre o *handset* e a estação base. Versões diferentes do algoritmo são usadas em diferentes países, e as duas mais comuns (A5/1 e A5/2) foram encontradas por engenharia reversa e publicadas por Briceno [BRICENO+03], [BRICENO+04]. Ambos os algoritmos também foram quebrados.

Shamir, Biryukov e Wagner [SHAMIR+] descobriram três possíveis ataques criptanalíticos ao A5/1 que renderiam resultados efetivos e poderiam ser alcançados em PC´s modernos em apenas alguns segundos. Em ambos os ataques, um PC pode captar a chave de uma conversação ainda no início da comunicação.

Muito embora a norma GSM permita o uso de algoritmos diferentes do COMP128, até agora a SDA (*Smartcard Developer Association*) ainda não encontrou uma rede sequer que tivesse adotado outra opção, nem mesmo nos EUA. A falha descoberta pode ser corrigível, porém pode ser apenas a primeira de uma família de vulnerabilidades correlatas. Não se pode produzir contramedidas de imediato sem que se conheça adequadamente o potencial de existirem outros pontos fracos no esquema do GSM.

Embora se estude mudar o padrão de criptografia mundial para o assim chamado A5/3, semelhante ao original (mas sem a vulnerabilidade que leva à possibilidade de quebrá-lo), o bug não foi corrigido no GSM atual. O algoritmo de encriptação A5/3 provê proteção de sinalização, de forma que informações sensíveis como números de telefone são protegidas em cima da trajetória de rádio, e proteção de dados de usuário, para proteger as chamadas de voz e outros usuários que geraram dados ignorando o caminho de rádio [ANTIPOLIS2002].

Capítulo 5

Redes *Wireless* LAN

De acordo com [SWAMINATHA+2002], uma rede local sem fios (WLAN) é um sistema de comunicação de dados promovendo uma extensão, ou alternativa para uma rede cabeada. As WLAN utilizam uma variedade de mecanismos de comunicação que substituem o cabeamento tradicional de uma rede; elas possuem transmissores, receptores e um portador nos quais os dados são modulados, que permitem a transmissão e recepção desses dados pelo ar e minimizam a necessidade da conectividade de cabos entre dispositivos.

As tecnologias de redes sem fio destinadas ao uso em *Wireless* LANs (*Local Area Networks*) foram padronizadas pelo IEEE (*The Institute of Electrical and Electronics Engineers, Inc*) através do grupo 802.11. O objetivo dessa padronização era definir um nível físico para redes onde as transmissões são realizadas na freqüência de rádio (RF) ou infravermelho (IR), e um protocolo de acesso ao meio.

5.1 A Tecnologia WLAN 802.11

O padrão IEEE 802.11 foi projetado com o intuito de suportar médio-alcance, taxas de aplicações de dados mais altas e endereçar estações móveis e portáteis. As estações móveis acessam a LAN quando estão em movimento e as estações portáteis se movem de local para local e somente são usadas enquanto estiverem numa localização física fixa.

Algumas versões do padrão 802.11 utilizam a técnica de modulação FHSS (*Frequency Hopping Spread Spectrum*) para a transmissão de dados, com ciclos rápidos entre as freqüências, e outras, a técnica DSSS (*Direct Sequence Spread Spectrum*), a mesma dos celulares CDMA: a transmissão ocorre em todas as freqüências simultaneamente.

O 802.11 é o padrão original de WLAN adotado em 1997 e suporta transmissões *wireless* de 1Mbps a 2Mbps, mas também existem outros padrões estabelecidos, que são [MCFARLAND+2003], [VINES2002]:

- **IEEE 802.11a** – é uma extensão do padrão original de LANs sem fio 802.11. Permite atingir taxas de transmissão de até 54 Mbps na banda de 5Ghz, utilizando a técnica

OFDM (*Orthogonal Frequency Division Modulation*) para minimizar a interferência causada pelos sinais refletidos nas paredes.

- **IEEE 802.11b** - é uma extensão do padrão LANs sem fio 802.11 e é baseado na versão DSSS do 802.11. Utiliza técnicas melhores de modulação, aumentando a capacidade até o máximo de 11 Mbps numa faixa de 2,4 GHz. Quando essa tecnologia é usada para redes de acesso à Internet, são denominadas redes Wi-Fi (*Wireless Fidelity*[6]).
- **IEEE 802.11d** – é um grupo global de harmonização. Diferentes países têm diferentes partes de banda de 2,4 e 5 GHz disponíveis para não autorizar redes *wireless*. 80211d busca ajudar a criar padrões que poderão ser aprovados na maioria dos países possíveis.
- **IEEE 802.11e** – é a última especificação IEEE rascunhada para redes sem fio com o intuito de fornecer características de qualidade de serviço e suporte multimídia aos ambientes sem fio doméstico e de negócios.
- **IEEE 802.11f** – é recomendado para práticas de comunicação entre pontos de acesso. Está quase completado.
- **IEEE 802.11g** - é um novo padrão IEEE que se aplica às LANs sem fio. 802.11g oferece transmissão sem fio, relativamente, a pequenas distâncias, com velocidades de 20 Mbps até 54 Mbps numa banda de 2,4 GHz, comparadas com 11 Mbps do padrão 802.11b. O 802.11g deixou de ser apenas uma especificação de rede *wireless*; agora, ele é um padrão oficial do IEEE. A oficialização do IEEE vinha sendo esperada há algum tempo, uma vez que vários fabricantes de equipamentos *wireless* já estavam desenvolvendo produtos com o 802.11g. O primeiro rascunho do 802.11g foi anunciado em novembro de 2001.
- **IEEE 802.11h** – melhorias do 802.11 para auxiliar a regularização das conformidades na Europa. Está quase completado.
- **IEEE 802.11i** – será o próximo nível de segurança para 802.11. Inclui a gerência e distribuição de chaves, encriptação e autenticação; ainda está em debate.
- **IEEE 802.11j** – é o equivalente ao 802.11h para o ambiente de regularização japonês.
- **IEEE 802.11k** – um projeto iniciado recentemente para padronizar a maneira como as redes 802.11a, b e g relatam as medidas de radio e as condições de rede para outras partes da pilha de rede e novas aplicações. Isso seria ideal para a administração da rede e para a detecção de falhas.

[6] Wi-Fi é a abreviatura de "*wireless* fidelity" (fidelidade sem fios) e é utilizado para descrever produtos que respeitam o conjundo de normas 802.11 criado pelo Electrical and Electronic Engineers (IEEE).

Em abril de 2002, o IEEE publicou um novo padrão sem fio 802, chamado IEEE *Broadband Wireless Access* (802.16 [IEEE]). Ele foi projetado para as redes metropolitanas sem fio (*Broadband Wireless Metropolitan Area Networks* ou *Wireless*MAN), objetivando a implantação de sistemas de acesso fixo em banda larga (*fixed* BWA - *Broadband Wireless Access*). O 802.16 utiliza tecnologias como WLL (*Wireless Local Loop*) / LMDS (*Local Multipoint Distribution System*) para estabelecer sistemas de distribuição de serviços de voz, dados, Internet e vídeo em banda larga, usando uma arquitetura similar à das redes celulares (acesso fixo). Normalmente, usa faixas situadas entre 10 e 66 GHz. No tocante a segurança, assim como o 802.11, o padrão 802.16 admite criptografia na camada de enlace dos dados.

Apesar dos diversos padrões 802.11 existentes e já citados, o destaque das próximas subseções será a tecnologia 802.11b para redes WLAN.

5.1.1 Arquitetura

A arquitetura adotada pelos padrões IEEE 802.11 para as redes sem fio é baseada na divisão da área coberta pela rede em células. As células são chamadas *BSA (Basic Service Area)*; um grupo de estações se comunicando por radiodifusão ou infravermelho em uma BSA constitui um BSS (*Basic Service Set*) e as estações de trabalho que se comunicam entre si dentro da BSS são as STA (*Stations*). A coordenação da comunicação entre as STA dentro da BSS é feita pelo AP (*Access Point*), que funciona como uma "ponte" entre a rede *wireless* e a rede tradicional. A coleção de todas as células BSS vizinhas que se interceptam e cujos AP (*Access Point*) estão conectados a uma mesma rede tradicional é chamada de ESS (*Extended Service Set*).

O padrão IEEE 802.11 permite que os dispositivos estabeleçam redes ponto-a-ponto ou redes baseadas num ponto de acesso fixo (AP) onde os nós móveis possam se comunicar. Conseqüentemente, o padrão define duas topologias básicas [KARYGIANNIS+2002]:

***Infrastructure mode*:** quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS). Na Figura 21, cada cliente envia todos os seus pacotes para uma estação central, ou *access point* (AP), que funciona como uma ponte *ethernet*, repassando adiante os pacotes para as redes apropriadas, com ou sem fios.

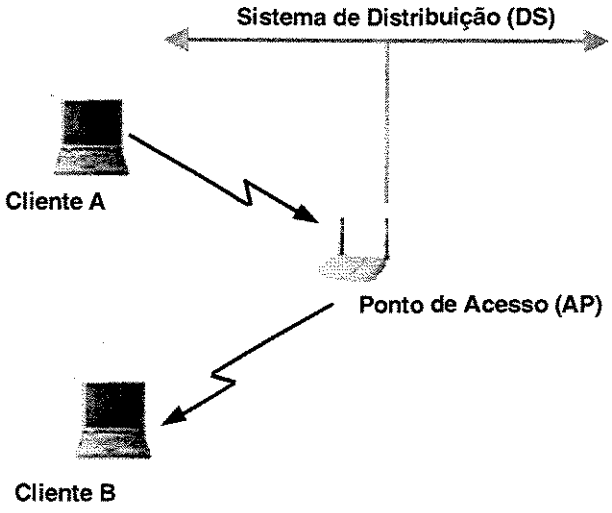


Figura 22 - Modo de Infra-estrutura

Ad hoc mode: quando não existe AP e as estações comunicam-se entre si diretamente. Cada cliente se comunica diretamente com os outros clientes dentro da rede, conforme a Figura 22. Somente os clientes dentro do alcance de transmissão (dentro da mesma célula) de cada cliente podem se comunicar entre si através desse modo. Se um cliente ad hoc deseja se comunicar com um cliente fora da célula, um membro da célula deve agir como um *gateway* e fazer o roteamento. Este modo não é recomendado pelo padrão.

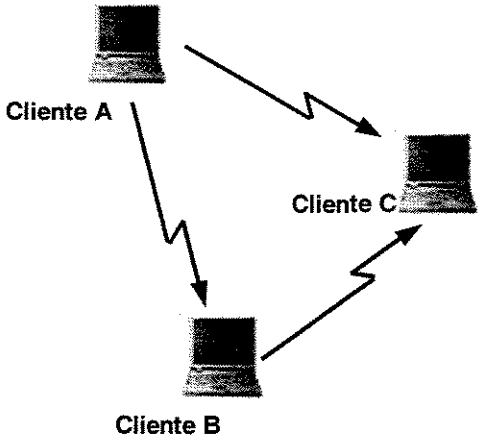


Figura 23 - Modo Ad hoc

Um ambiente de WLAN tem estações de clientes sem fios que usam modem de rádio para se comunicar a um AP. As estações de cliente, geralmente, são equipadas com um cartão de interface de rede sem fios (WNIC) que consiste no modem de rádio e na lógica para interagir com a máquina do cliente e o software. Um AP inclui, essencialmente, um modem de rádio de um

lado e uma ponte para a conexão no outro. Todas as comunicações entre as estações de cliente e os clientes e a rede passam pelo AP. A topologia básica de uma WLAN é vista na Figura 23:

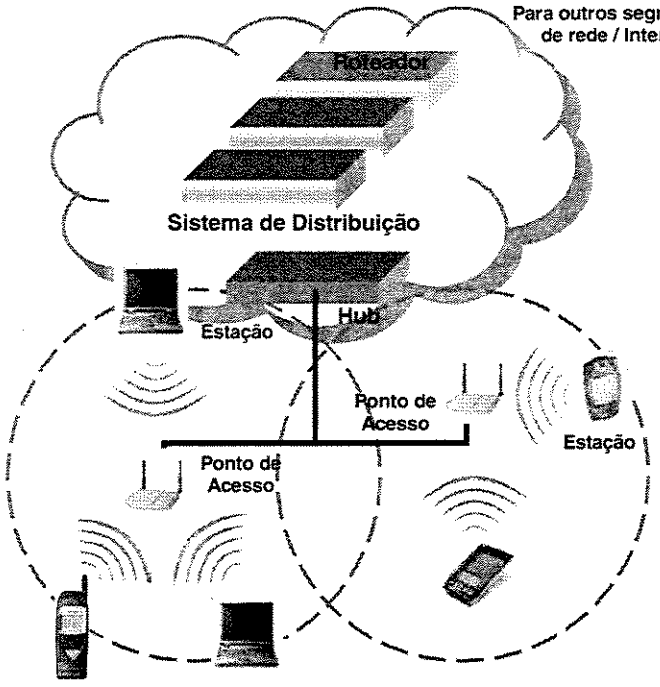


Figura 24 - Topologia da Wireless LAN 802.11

As WLAN compreendem dois tipos de equipamentos: uma estação *wireless* e um ponto de acesso. Uma estação, ou cliente, é tipicamente um *laptop* ou um computador pessoal notebook (PC) com um cartão de interface de rede *wireless* (NIC). Um *laptop* e um *notebook* sem fios, com tecnologia sem fios habilitada, são idênticos aos *laptops* e *notebook*, com exceção que eles usam NICs sem fios para se conectar a pontos de acesso na rede. O NIC sem fios é comumente inserido no *slot* PCMCIA (*Personal Computer Memory Card International Association*) do cliente ou na porta USB (*Universal Serial Bus*). Eles usam freqüências de rádio ou raios infravermelhos para estabelecer conexões com a WLAN. O AP, que age como uma ponte entre a rede sem fios e a rede tradicional, tipicamente inclui um rádio, uma interface de rede como 802.3 e um software de comunicação, e funciona como uma estação básica para a rede sem fios, agregando múltiplas estações sem fios na rede tradicional.

A distância de cobertura segura para WLAN 802.11 depende de vários fatores, incluindo a taxa de dados requerida e a capacidade, fontes de interferência de RF, área física e características, potência, conectividade e uso de antena.

Distâncias teóricas vão de 29 metros (para 11Mbps) em uma área de escritório

fechado para 485 metros (para 1Mbps) em uma área aberta. Porém, a distância típica para conectividade de um equipamento 802.11 é aproximadamente 50 metros (aproximadamente 163 pés) em lugar fechado e, ao ar livre, com uma antena omni-direcional, a conectividade pode ser aumentada em 400 metros.

Os APs, exercendo a função de "ponte", podem conectar duas ou mais redes juntas e lhes permitir comunicação, envolvendo uma configuração ponto-a-ponto ou multiponto. Numa arquitetura ponto-a-ponto, duas LANs são conectadas uma a outra através dos respectivos APs das LANs. No caso de multiponto, uma subrede de uma LAN é conectada a várias outras subredes em outra LAN via cada subrede AP. Por exemplo, se um computador numa subrede A precisar se conectar com computadores das subredes B, C e D, o AP da subrede A deverá se conectar com aos respectivos APs de B, C e D.

5.1.2 Benefícios

O método de comunicação das WLAN está se tornando muito atraente nos dias de hoje, podendo resultar em aumento de eficiência e redução de custos. As WLAN oferecem quatro benefícios aos usuários [KARYGIANNIS+2002], [SWAMINATHA+2002]:

Mobilidade: os usuários podem ter acesso a arquivos, recursos de rede e à Internet sem ter que se conectar fisicamente a rede com fios. Eles podem ser móveis, já que retêm alta velocidade e tempo real de acesso a LAN.

Rápida Instalação: o tempo requerido para instalação é reduzido porque as conexões de rede podem ser feitas sem a movimentação ou adição de fios, ou sem passá-los por paredes ou tetos.

Flexibilidade: empreendimentos podem desfrutar da flexibilidade de instalação das WLAN; pequenas WLAN podem ser instaladas rapidamente para necessidades temporárias.

Escalabilidade: a topologia de rede WLAN pode ser facilmente configurada para reconhecer uma aplicação específica.

Devido aos benefícios fundamentais, o mercado de WLAN tem aumentado continuamente durante os últimos anos, e as WLAN ainda estão ganhando em popularidade. De acordo com o IDC (*International Data Corporation*), o número de subscritores móveis ultrapassará 500 milhões no mundo, antes de 2002. O órgão também aposta que as vendas de tecnologia WLAN alcançarão $3.2 bilhões antes de 2005. WLAN

estão se tornando uma alternativa viável em soluções sem fios tradicionais. Na realidade, hospitais, universidades, aeroportos, hotéis e lojas de especialidade estão oferecendo acesso WLAN à Internet.

5.1.3 Segurança

A especificação IEEE 802.11 identificou vários serviços para proporcionar um ambiente operacional seguro. Os serviços de segurança são alcançados, em grande parte, pelo protocolo WEP (*Wired Equivalent Privacy*), utilizado para proteger dados em nível de ligação durante a transmissão sem fios entre os clientes e os pontos de acesso. Quer dizer, WEP não provê segurança fim-a-fim, mas somente para a porção sem fios da conexão. Um exemplo de segurança pode ser notado na Figura 24:

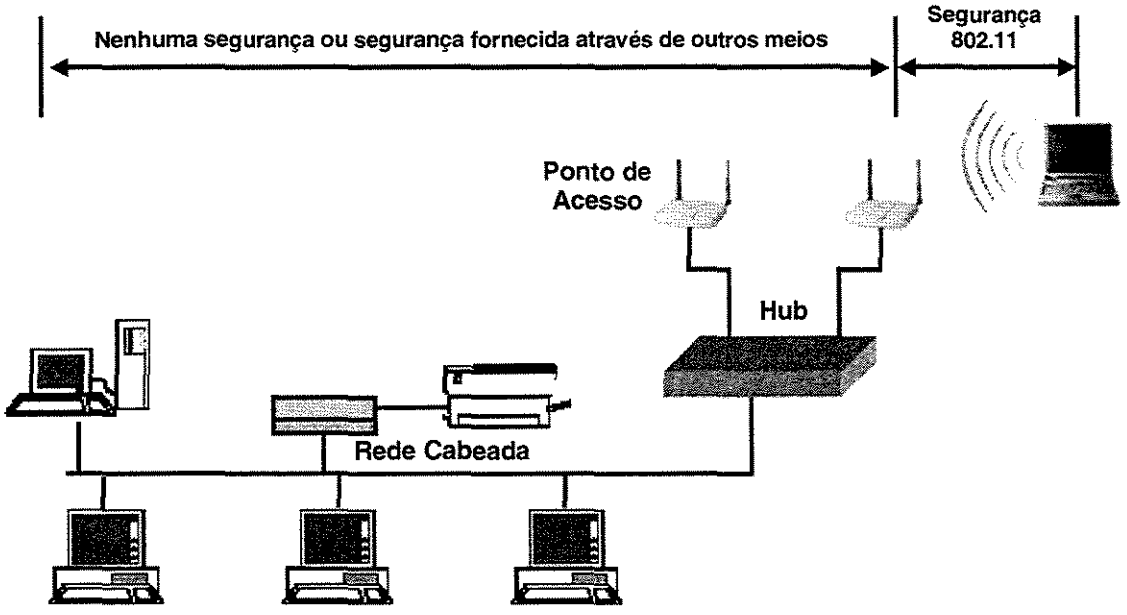


Figura 25 - Segurança sem fios de 802.11 numa rede típica

Os três serviços de segurança básicos definidos pelo IEEE para o ambiente de WLAN são:

Autenticação: a meta primária do protocolo WEP é prover um serviço de segurança para verificar a identidade da comunicação das estações cliente; tudo isso para controlar o acesso à rede e negá-lo às estações cliente que não possam se autenticar corretamente.

Confidencialidade: confidencialidade ou privacidade é a segunda meta de WEP. Ele foi desenvolvido para alcançar privacidade em uma rede sem fios. A intenção é prevenir a informação de um possível ataque passivo (um "espiar" casual).

Integridade: um terceiro objetivo do protocolo WEP é o serviço de segurança que assegure que as mensagens não serão modificadas em trânsito entre os clientes sem fio e os pontos de acesso, num ataque ativo.

Vale a pena salientar que existem outros serviços de segurança de grande importância, como auditoria, autorização e não-repúdio.

5.1.3.1 *Wired Equivalent Privacy* (WEP)

O protocolo WEP é definido pelo padrão IEEE 802.11 como um esquema opcional de encriptação que inclui mecanismos de segurança para os fluxos de dados em *wireless* LAN. Ele se baseia numa chave secreta compartilhada entre as estações para proteger o corpo da mensagem transmitida e, ambas a chave e o algoritmo, são usados para a encriptação e decriptação dos dados.

No processo de encriptação, primeiramente, o *integrity checksum* da mensagem é calculado e concatenado com a mensagem, para se obter um texto plano que será utilizado como entrada numa fase seguinte.

Em seguida, o texto plano é encriptado utilizando-se o algoritmo RC4 (*Rivest Code* 4) e escolhendo-se um vetor de inicialização (IV). O algoritmo gera então uma longa seqüência pseudo-aleatória (PRNG), como função do IV e da chave K. Sobre esta seqüência, é feito um exclusive-*or* com o texto plano para a obtenção da mensagem cifrada. Finalmente, é transmitido o IV e o texto cifrado pelo link de rádio [VINES2002]. A Figura 25 mostra o algoritmo WEP de encriptação.

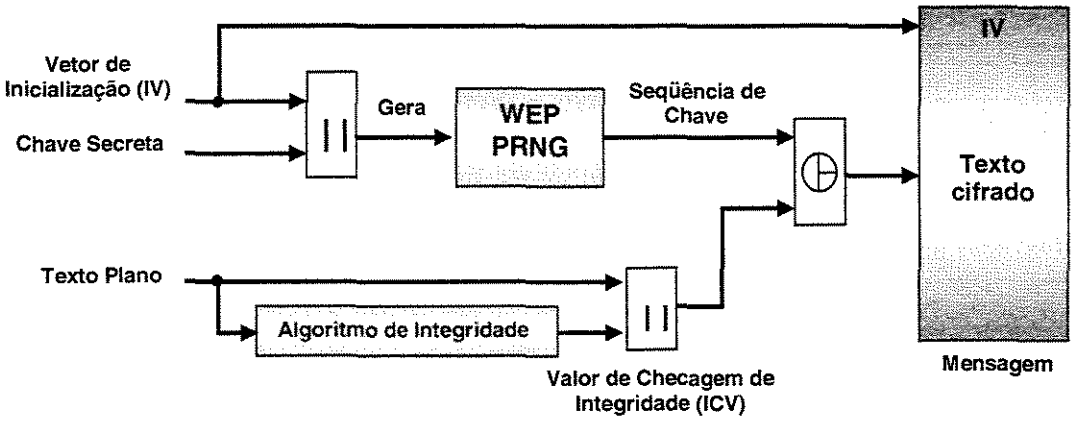


Figura 26 - Algoritmo de Encriptação WEP

A decriptação do fluxo de dados, pelo protocolo WEP, é feita da seguinte maneira:

- O IV da mensagem entrante é usado para gerar a seqüência de chave necessária para sua decifragem.
- O texto cifrado, combinado com a própria seqüência de chave, produz o texto plano original e o ICV.
- A decriptação é verificada executando o algoritmo de checagem de integridade no texto plano recuperado e comparando a saída ICV1 com o ICV transmitido com a mensagem.
- Se ICV1 não for igual a ICV, a mensagem recebida está errada, e uma indicação de erro é retornada à estação que a enviou. Unidades móveis com mensagens errôneas não são autorizadas.

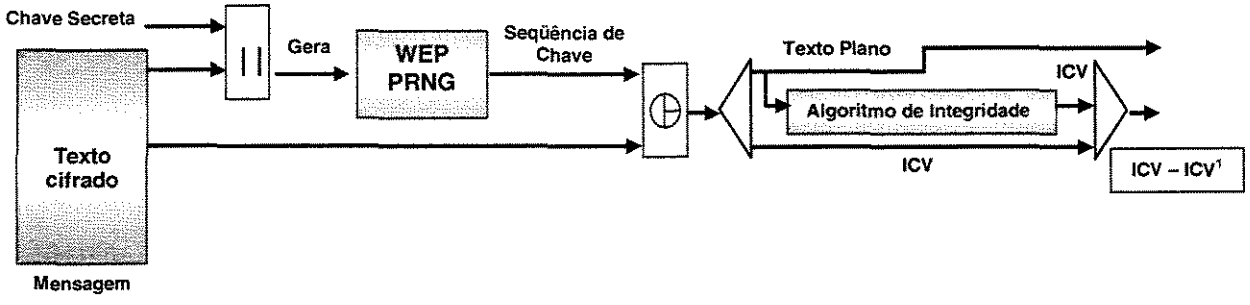


Figura 27 - Algoritmo de Decriptação WEP

5.1.3.2 Autenticação do Cliente Móvel

A especificação IEEE 802.11 define duas maneiras de validar os usuários sem fios que tentam ganhar acesso às redes sem fios. Uma maneira está baseada na criptografia e a outra não. Para o modo não-criptografado, há duas maneiras diferentes para identificar um cliente sem fios tentando se acoplar à rede. Porém, ambos os modos são base de identificação para os mecanismos de verificação. As estações sem fios pedindo acesso simplesmente respondem com o Serviço de Identificador Fixo (SSID – *Service Set Identifier*) para a rede sem fios – isso não é uma verdadeira "autenticação". Os dois modos estão referenciados como autenticação de Sistema Aberto e autenticação de Sistema Fechado. Uma taxonomia das técnicas para 802.11 é descrita na Figura 27.

No sistema aberto, um cliente é autenticado se simplesmente responder com uma *string* vazia para o SSID - conseqüentemente, o nome "autenticação NULA". Com o segundo método, autenticação fechada, os clientes sem fios têm que responder com o SSID atual da rede sem fios. Quer dizer, um cliente tem acesso permitido se responder com a *string* correta de 0-byte a 32-bytes que identifica o BSS da rede sem fios. Novamente, este tipo primitivo de autenticação é só um esquema de identificação; na prática, nenhum desses dois esquemas oferece segurança robusta contra acessos sem autorização. Eles são altamente vulneráveis contra ataques e, sem encarecimentos, convidativos a incidentes de segurança.

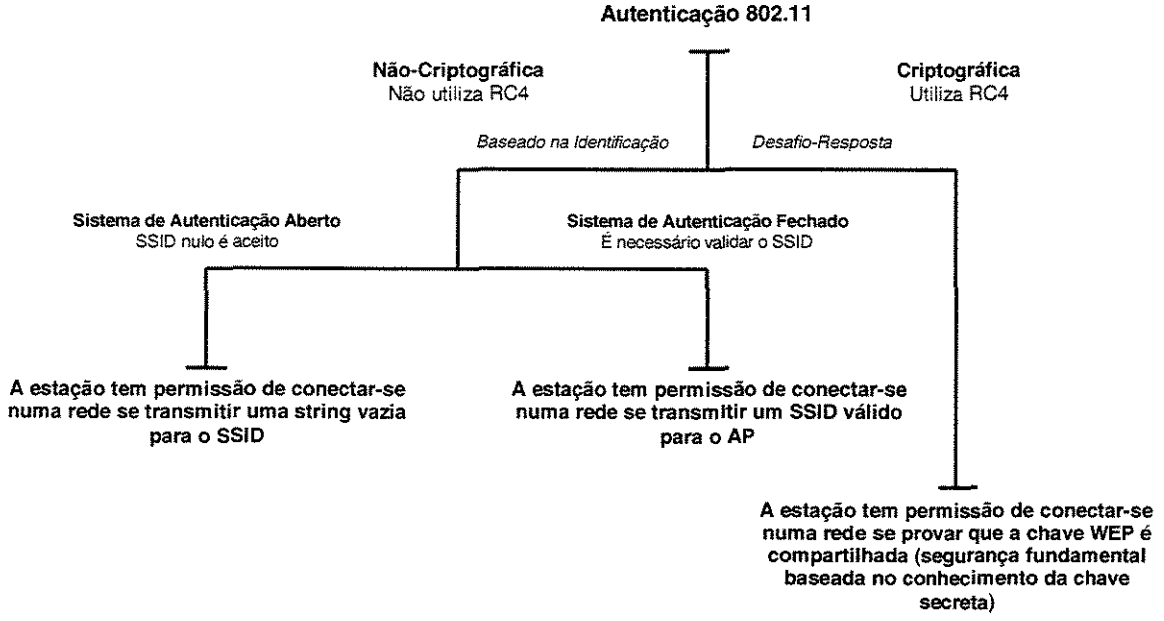


Figura 28 - Uma Taxonomia das Técnicas de Autenticação das Redes 802.11

Uma técnica criptográfica para autenticação é a autenticação de chave compartilhada. É um simples esquema de "desafio-resposta" baseado na possibilidade de um cliente ter conhecimento de um segredo compartilhado. Neste esquema, como descrito na Figura 28, um valor randômico é gerado pelo ponto de acesso e enviado ao cliente sem fios. O cliente, usando uma chave criptográfica (chave WEP) que é compartilhada com o AP, codifica esse valor e retorna o resultado para o AP. O AP decifra o resultado computado pelo cliente e só permite o acesso se o valor decifrado estiver igual ao valor randômico transmitido. O algoritmo usado na computação criptográfica é o RC4, e o método de autenticação descrito é justamente uma técnica criptográfica rudimentar, pois não provê autenticação mútua. Isso quer dizer que o cliente não autentica o AP e então, não tem nenhuma garantia que esse cliente está se comunicando com um legítimo AP e a rede sem fios.

5.1.3.3 Privacidade

O padrão 802.11 suporta a privacidade (confidencialidade) através do uso de técnicas criptográficas para interfaces sem fios. A técnica criptográfica WEP para confidencialidade também usa a chave-simétrica RC4, algoritmo de cifragem que gera uma seqüência de dados pseudo-randômicos. Através da técnica WEP, os dados podem ser protegidos da revelação, durante a transmissão, pelo *link* sem fios; o WEP é aplicado a todos os dados sobre as camadas de redes 802.11 para proteger tráfegos como o TCP/IP (*Transmission Control Protocol / Internet Protocol*), IPX (*Internet Packet Exchange*) e HTTP (*Hyper Text Transfer Protocol*).

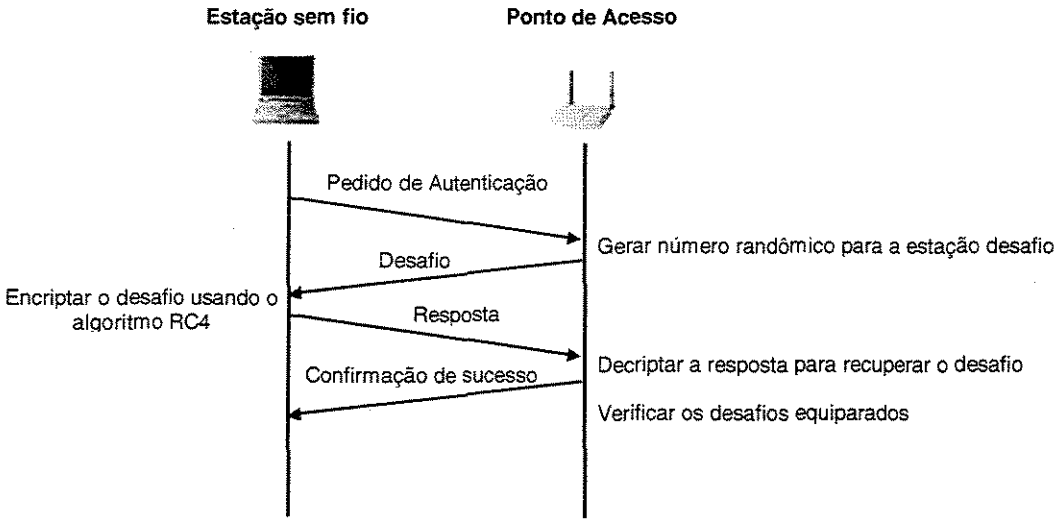


Figura 29 - Fluxo de Autenticação de Mensagem de uma Chave Compartilhada

O WEP suporta chaves criptográficas de tamanhos de 40 *bits* a 104 *bits*. Por exemplo, a chave WEP de 104 *bits*, com IV de 24 *bits*, se torna uma chave RC4 de 128 *bits*. Em geral, aumentando o tamanho das chaves, aumenta-se a segurança da técnica criptográfica. Para chaves de 80 *bits*, o número de chaves possíveis excede a potência dos computadores. Na prática, a maioria dos desenvolvimentos de WLAN gira em torno de chaves de 40 *bits*. Além disso, ataques recentes mostraram que a aproximação do WEP para a privacidade é, infelizmente, vulnerável a certos ataques, não importando o tamanho das chaves.

A privacidade de WEP é ilustrada na Figura 29.

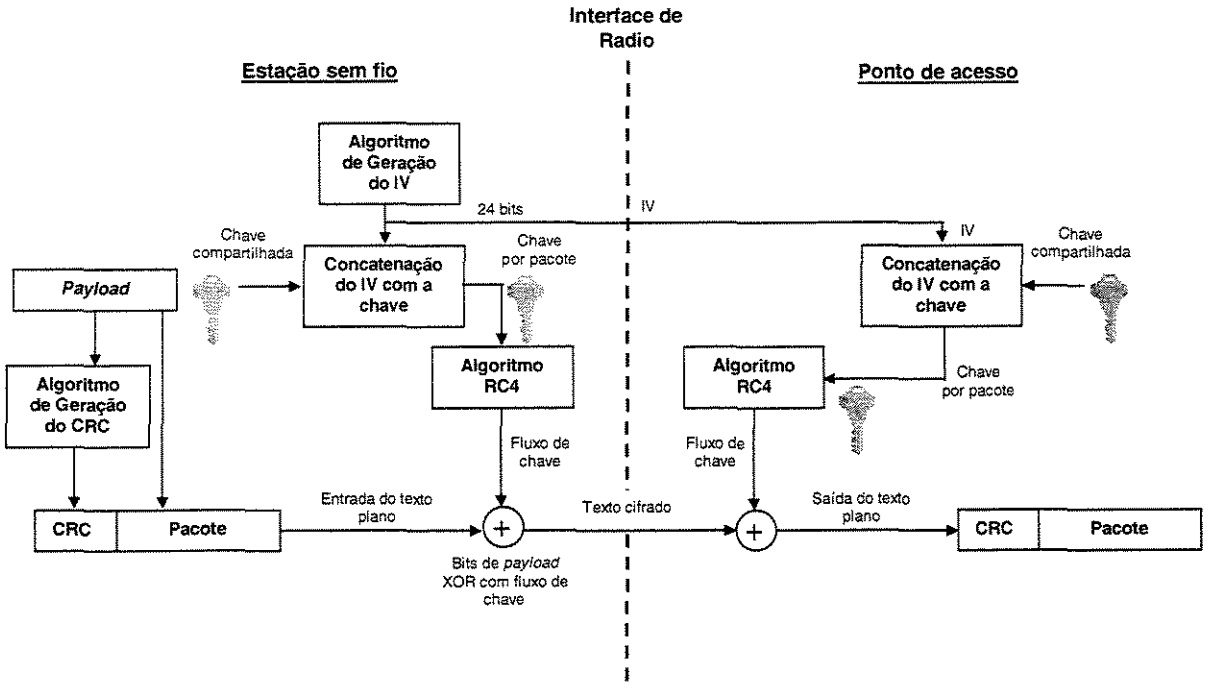


Figura 30 - Privacidade WEP usando Algoritmo RC4

5.1.3.4 Integridade

A especificação IEEE 802.11 também esboça meios de prover integridade dos dados para mensagens transmitidas entre os clientes sem fios e os pontos de acesso. Este serviço de segurança foi projetado para rejeitar qualquer mensagem que tenha sido alterada por um adversário ativo no meio de comunicação. Esta técnica usa uma simples aproximação codificada de Verificação de Redundância Cíclica (CRC – *Cyclic Redundancy Check*). Como descrito no diagrama acima, um CRC-32, ou uma seqüência de verificação é computada em cada carga útil antes da transmissão. O pacote com "integridade marcada" é então codificado usando a chave RC4 para prover a mensagem de texto cifrado. No final do receptor, a decriptografia é executada e o CRC é recomputado na mensagem que é recebida. O CRC computado no fim do receptor é comparado com aquele da mensagem original. Se os CRCs não se igualarem, houve uma violação de integridade (um *spoofer* de mensagem ativo), e o pacote é descartado. Com os serviços de privacidade, infelizmente, a integridade da 802.11 é vulnerável a certos ataques.

A especificação IEEE 802.11 não faz, infelizmente, identificação de meios de administração da chave (ciclo de vida de manutenção da chave criptográfica). Novamente, a administração da chave (provavelmente o aspecto mais crítico de um sistema de

criptografia) para 802.11 é um grande exercício para os usuários da rede 802.11; talvez, indivíduos não estão totalmente cientes de sua importância, o que pode acarretar a introdução de vulnerabilidade no ambiente de WLAN. Estas vulnerabilidades incluem chaves de WEP que não são únicas, que nunca são modificadas, ou chaves fracas (todos zeros, todos uns, baseados em senhas facilmente adivinhadas, ou outros padrões triviais semelhantes).

5.1.4 Problemas de Segurança com o padrão IEEE 802.11

A base das WLAN é o uso do protocolo WEP. Esse protocolo usa o algoritmo criptográfico RC4 com uma chave de comprimento variável para proteger o tráfego. Novamente, os padrões 802.11 suportam chaves criptográficas WEP de 40 *bits* e as chaves são baseadas em senhas escolhidas pelos usuários, o que reduz efetivamente o tamanho das chaves.

Alguns problemas relativos ao comprometimento da segurança nas redes WLAN, por parte de usuários maliciosos, foram detectados, destacando-se os ataques passivos para decifrar tráfegos baseados em análises estatísticas, ataques ativos para injetar novo tráfego em estações móveis sem autorização, ataques ativos para decifrar tráfego (baseado em enganar o ponto de acesso) e ataques de construção de dicionários (o ataque de construção de dicionários só é possível depois de analisado o tráfego de um dia inteiro).

Ocorrem vários problemas com o protocolo WEP, incluindo [KARYGIANNIS+2002], [WALKER2000]:

1. O uso de chaves estáticas WEP – muitos usuários, numa rede sem fios potencial, compartilham uma mesma chave idêntica por longos períodos de tempo, caracterizando uma vulnerabilidade de segurança. Isso ocorre, em parte, devido à vulnerável falta de administração da chave no protocolo WEP. Por exemplo, se um *laptop* for perdido ou roubado, a chave poderia comprometer todos os outros que compartilham aquela chave e, além disso, desde que todas as estações usam a mesma chave, uma grande quantidade de tráfego pode rapidamente estar disponível para ataques analíticos.
2. O vetor de inicialização (IV) em WEP, como mostrado na Figura 29, é um campo de 24 *bits* enviado dentro de um pedaço de texto numa mensagem. A *string* 24 *bits*, usada para inicializar o fluxo da chave gerada pelo algoritmo RC4, é um campo relativamente pequeno quando usado para propósitos criptográficos. O

reuso do mesmo vetor de inicialização (IV) produz fluxos de chaves idênticos para a proteção dos dados, e vetores curtos garantem que estes serão repetidos depois de um tempo pequeno, numa rede ocupada. O padrão 802.11 não especifica como os vetores são criados ou modificados e nem como os NICs individuais sem fios possivelmente usam um vetor de inicialização constante, o que resulta na possibilidade dos *hackers* registrarem o fluxo de redes, determinarem o fluxo das chaves e usarem tudo isso para decifrar um texto cifrado.

3. O vetor de inicialização (IV) compõe uma parte da chave de encriptação do RC4. Um intruso, conhecendo os 24 *bits* de todo o pacote de chaves, combinada com uma fraqueza no algoritmo RC4, executa um ataque analítico, recuperando a chave depois de analisar e interceptar somente uma pequena quantidade de tráfego.
4. WEP não fornece proteção de integridade criptográfica; porém, o protocolo MAC de 802.11 usa um CRC não-criptográfico para checar a integridade dos pacotes, e reconhecer pacotes com *checksum* correto. A combinação de *checksum* não-criptografado com o fluxo de cifras é extremamente perigosa e freqüentemente conduz a ataques não intencionais do lado do canal, como ocorre em WEP. Isso exemplifica um ataque ativo, onde o atacante decifra qualquer pacote, modifica-o, o CRC envia-o ao AP e notifica se o pacote é reconhecido. Esses tipos de ataques são sutis e por isso, é arriscado projetar protocolos de encriptação que não incluam proteção de integridade criptográfica, devido à possibilidade de interação com outros níveis de protocolo que podem dar informações sobre o texto cifrado.

5.1.5 Ataques ao Protocolo WEP

Uma série de investigações constatou a existência de casos reais de ataques ao protocolo WEP, dentre eles [STUBBLEFIELD+2001]:

- A Universidade da Califórnia, Berkeley, publicou uma documentação sobre a vulnerabilidade do reuso do fluxo de chave causada pela má administração dos IVs [BORISOV+2001]. Essa vulnerabilidade permite que um atacante capture dois pacotes criptografados usando o mesmo fluxo de chave, mas não decifre os seus conteúdos; eles também conseguem inserir ou modificar o tráfego, redirecionar o tráfego decifrado para um endereço IP alternativo, ou até mesmo

devolver o dicionário IV utilizado para decifrar todo e qualquer conteúdo que trafega na rede sem fios.

- Em 2000, Scott Fluher, Itsik Mantin e Adi Shamir expuseram duas significantes debilidades do RC4 no algoritmo de programação de chave (KSA). Eles descobriram que uma pequena porção da chave secreta determina uma grande porção do resultado de KSA inicial, e também uma falha inerente em WEP: que a chave secreta pode ser facilmente derivada considerando a chave secreta usada com múltiplos IVs [FLUHRER+2001].
- Em 2001, Nikita Borisov e um grupo de pesquisadores da Universidade da Califórnia, Berkeley, relataram as fraquezas encontradas no fluxo de cifras do WEP RC4. Eles descobriram que, se duas mensagens usarem o mesmo fluxo de chave, informações de ambas as mensagens poderiam ser reveladas [BREWER+].

Após a disponibilização de documentos que relatavam as vulnerabilidades do WEP, ferramentas para a automatização da quebra de chaves WEP foram criadas para facilitar a tarefa: AirSnort e WEPCrack.

O AirSnort é uma boa ferramenta de quebra de chaves WEP; ela captura pacotes "interessantes" que serão analisados posteriormente. Após a captura de um número suficiente de pacotes, o processo de quebra é iniciado. De acordo com a documentação da ferramenta, são necessários aproximadamente 1500 pacotes "interessantes" para quebrar uma chave WEP de 128 *bits*. A criptografia WEP utiliza um vetor de inicialização RC4 para criptografar pacotes com chaves diferentes. Primeiramente, isso parece seguro. O problema é que o vetor de inicialização (IV), além de ser incrementado seqüencialmente, possui 24 *bits*, ou seja, a cada 2^{24} pacotes, o IV se repete (este é o pacote interessante). 2^{24} pacotes significam 16,8 milhões de pacotes que são obtidos em uma rede de 5 Mbps congestionada durante algumas horas.

O WEPCrack é outra ferramenta disponível na Internet utilizada para decodificar pacotes, identificar pacotes fracos e quebrar a chave WEP.

5.1.6 Contra-Medidas de Segurança para as Redes 802.11

De acordo com os itens expostos acima, notamos que os objetivos do protocolo WEP foram quebrados, o que significa que uma rede que utiliza o WEP não é segura, devendo então considerá-la uma rede pública como a Internet.

Uma solução freqüente para provar segurança nas redes 802.11 é colocar a rede sem fio atrás do *firewall*, só que, uma vez que se tem acesso facilmente a rede através do AP, o adversário estará indiretamente quebrando a segurança do *firewall*. O ideal seria colocar o AP fora do *firewall* e utilizar mecanismos de segurança secundários de autenticação, como a implementação de um VPN (*Virtual Private Network*) com, por exemplo, IPSec (*Secure Internet Protocol*).

O VPN é uma tecnologia utilizada para proporcionar transmissões de dados seguras nas infra-estruturas de redes públicas. Técnicas criptográficas são empregadas para proteger a informação do IP (*Internet Protocol*) quando ele passa de uma rede para outra.

A Figura 30 ilustra uma VPN para conectividade local-a-local; a comunicação do tráfego de um local A para o B é protegida conforme a movimentação pela Internet.

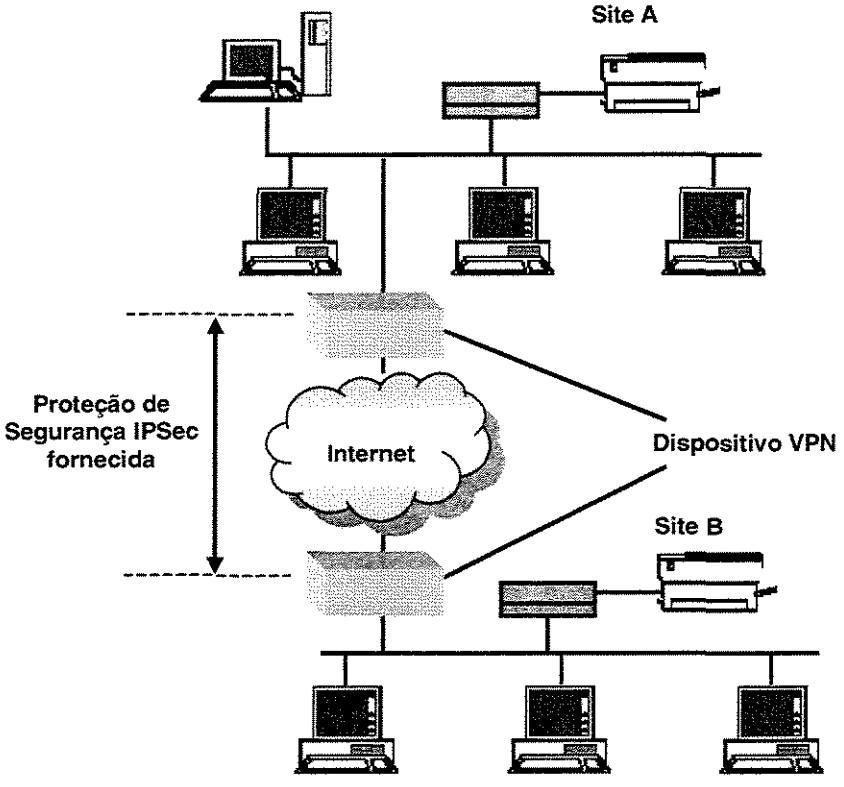


Figura 31 - Uso Típico do VPN para Comunicações de Internet Seguras

As VPNs utilizam o protocolo IPSec, que dispõem de um conjunto de algoritmos asseguram comunicações privadas nas redes IP. Em relação à segurança, o IPSec proporciona a confidencialidade, integridade de conexão, autenticação dos dados originais,

proteção repetida e proteção de análise do tráfego.

O IPSec executa a tarefa de barrar as mensagens por um túnel encriptado, através de dois cabeçalhos de IPSec especiais inseridos imediatamente depois do cabeçalho IP em cada mensagem. O cabeçalho ESP (*Encapsulating Security Protocol*) provê privacidade e protege contra modificações maliciosas, e o cabeçalho AH (*Authentication*) protege contra modificação sem privacidade.

O IKE (*Internet Key Exchange*) é um mecanismo que permite que chaves secretas e outros parâmetros de proteção relacionados sejam trocados antes da comunicação, sem a intervenção do usuário.

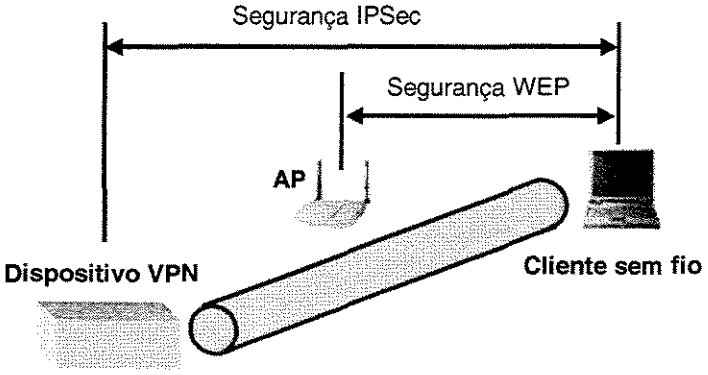


Figura 32 - Segurança do VPN em adição ao WEP

O uso do IPSec em WLAN é mostrado na Figura 31. O túnel IPSec é provido pelo cliente *wireless* através do AP para o dispositivo VPN, na extremidade da rede. Com o IPSec, os serviços de segurança ocorrem na camada de rede da pilha de protocolo, ou seja, todas as aplicações e protocolos que operam sobre aquela camada são protegidos pelo IPSec. O VPN codifica e protege os dados transmitidos de e para a rede cabeada.

Os serviços de segurança do IPSec são independentes da segurança ocorrida na camada 2 (camada de enlace de dados), que é a camada de atuação do WEP. Eles podem ser utilizados como adição ou substituição do WEP.

Observando as fragilidades do protocolo WEP, conclui-se que:

- O IV deveria ser longo e nunca se repetir durante a vida da chave secreta compartilhada, e nunca ser duplicado entre máquinas utilizando a mesma chave.
- Um código mais forte de autenticação de mensagens em vez do CRC que dependa da chave e do IV.

Como solução imediata, mas não definitiva e totalmente segura, para eliminar algumas vulnerabilidades do WEP, surgiu um novo protocolo chamado WEP2 ou TKIP (*Temporal Key Integrity Protocol*), primeira versão do WPA (*Wi-Fi Protected Access*). Foi projetado por membros da Wi-Fi Aliança e do IEEE empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA. Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 *bits*, ao invés de 24 como no WEP, e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação utiliza o 802.1x e o EAP (*Extensible Authentication Protocol*), que através de um servidor de autenticação central, faz a autenticação de cada usuário antes deste ter acesso a rede.

5.1.7 802.16: O Novo Padrão Sem Fio para Redes Metropolitanas (WMAN)

O novo padrão IEEE 802.16 [EKLUND+2002] com a sua interface aérea de *Wireless* MAN foi publicado em 8 de abril de 2002 e também é conhecido como "WiMAX". Ele possui uma área de cobertura muito maior que as redes padrão 802.11, chegando a 50 quilômetros de alcance, criando redes metropolitanas sem fio.

O padrão 802.16 usa freqüências de 10 GHz a 66 GHz para criação das redes metropolitanas sem fio e deve suportar aplicações multimídias como videoconferências, voz e jogos. Pela facilidade de integração com a tecnologia 802.11 de *Wireless* LAN, o 802.16 funciona como uma extensão de tecnologias de acesso à internet em banda larga, como ADSL ou cabo. Basta conectar o cabo ADSL, por exemplo, a um transmissor 802.16 para que ele envie o sinal para todos os equipamentos compatíveis com o padrão 802.11 a uma velocidade de transmissão de dados a até 70 Mbps (Megabits por segundo).

As tecnologias 802.11 e 802.16 são complementares, e resolvem problemas diferentes. Os ambientes em que as redes 802.11 e 802.16 operam são semelhantes em alguns aspectos, principalmente no fato de terem sido projetadas para fornecer comunicações sem fios de alta largura de banda. Entretanto, algumas diferenças existem entre os padrões: o 802.16 fornece serviço para edifícios, que não são móveis e grande

parte do 802.11 lida com mobilidade; o 802.16, criado para uso residencial e comercial, deverá dar suporte para tráfego em tempo real (aplicações multimídia), enquanto que o 802.11 não foi projetado para telefonia e uso pesado em multimídia.

Em síntese, o padrão 802.11 foi projetado para ser a Ethernet móvel e o 802.16, para ser uma rede de televisão a cabo sem fio, mas estacionária. As diferenças são tão grandes que os padrões resultantes são muito diferentes, pois eles procuram otimizar aspectos distintos das redes.

Um último aspecto importante das redes 802.16 é a segurança; mecanismos de autenticação, autorização e privacidades são essenciais e obrigatórios para a garantia da segurança na comunicação aberta sobre as redes metropolitanas sem fio.

Capítulo 6

Redes *Wireless* PAN

PANs são redes que focalizam ao redor de um indivíduo [SWAMINATHA+2002]. Livremente, uma PAN pode incluir um telefone celular, um PDA, e um *laptop* com tecnologia sem fios habilitada. Os três dispositivos comunicam-se um com o outro, formando uma rede PAN ad hoc. As redes ad hoc são um paradigma relativamente novo de comunicação sem fios, onde não há nenhuma infra-estrutura fixa como estações base ou pontos de acesso. Nessas redes, os dispositivos mantêm configurações de rede ocasionais formadas rapidamente, confiando num sistema de roteadores móveis se conectando através de ligações sem fios para permitir que dispositivos se comuniquem entre si. Os dispositivos dentro uma rede ad hoc controlam a configuração da rede, mantêm e compartilham recursos.

Redes ad hoc permitem que os dispositivos tenham acesso às aplicações sem fios, como sincronização de endereços e compartilhamento de arquivos, dentro de uma área de rede pessoal (PAN). Quando combinada com outras tecnologias, estas redes podem ser ampliadas para incluir acessos à rede e a Internet. Dispositivos *Bluetooth* que tipicamente não têm acesso aos recursos de rede, mas que são conectados numa rede *Bluetooth* com um dispositivo com capacidade 802.11, podem alcançar conexões dentro da rede incorporada, como também alcance fora para a Internet.

6.1 A Tecnologia *Bluetooth*

Em maio de 1998, um grupo de importantes empresas como Ericson, IBM, Intel, Nokia e Toshiba, formaram o *Bluetooth Special Interest Group* (SIG) [SAIRAM+2002] para coordenar o desenvolvimento e promover a tecnologia *Bluetooth*. É uma tecnologia que permite conexões sem fios entre quaisquer dispositivos de computação, comunicação e eletrônicos – e promete muito mais que isso, inclusive o reconhecimento e sincronização de dispositivos "inteligentes".

O *Bluetooth* facilita as conexões sem fios e de curto alcance, e as comunicações entre vários dispositivos eletrônicos; é um padrão aberto para rádio digital de alcance limitado. Possui baixo custo, baixo poder, e tecnologia de baixo perfil que provê um mecanismo para

criação de pequenas redes sem fio numa base ad hoc.

As redes ad hoc são fundamentadas, principalmente, na tecnologia *Bluetooth*. *Bluetooth* é considerado uma tecnologia WPAN e oferece transmissões rápidas e seguras para voz e dados; os dispositivos de *Bluetooth* eliminam a necessidade de cabos e provêm uma ponte para as redes existentes.

Bluetooth pode ser usado para conectar qualquer dispositivo a outro; como exemplo, podemos ter a conexão entre um PDA e um telefone móvel. A meta de *Bluetooth* é conectar dispositivos discrepantes (PDAs, telefones celulares, impressoras, faxes, etc.) juntos num ambiente sem fios pequeno. De acordo com os propósitos principais da tecnologia, *Bluetooth* é um padrão que vai eliminar conexões e cabos entre dispositivos estáticos e móveis, facilitar as comunicações de dados e voz e oferecer a possibilidade de sincronização entre dispositivos pessoais nas redes ad hoc.

Como toda rede ad hoc, as topologias de rede *Bluetooth* são estabelecidas numa base temporária e fortuita. Uma característica distinta de redes *Bluetooth* é a relação de mestre-escravo mantida entre os dispositivos de rede. Até oito dispositivos *Bluetooth* mantidos juntos na rede, num relacionamento mestre-escravo, chama-se *piconet* [SAIRAM+2002]. Em um piconet, um dispositivo é designado como o mestre da rede, com até sete escravos conectados diretamente àquela rede. É o mestre que controla e estabelece a rede. Os dispositivos, em um *piconet* de *Bluetooth*, operam no mesmo canal e seguem a mesma seqüência de saltos de freqüência. Embora somente um dispositivo seja mestre para cada rede, um escravo de uma rede pode agir como mestre para outras, assim criando uma cadeia de redes. Esta série de *piconets*, freqüentemente chamada de *scatternets* [SAIRAM+2002], permite que vários dispositivos possam ser interconectados acima de uma distância estendida. A topologia dinâmica também pode ser alterada durante qualquer sessão: como um dispositivo se move para, e longe do dispositivo mestre da rede, a topologia e, conseqüentemente, as relações dos dispositivos na rede imediata também mudam.

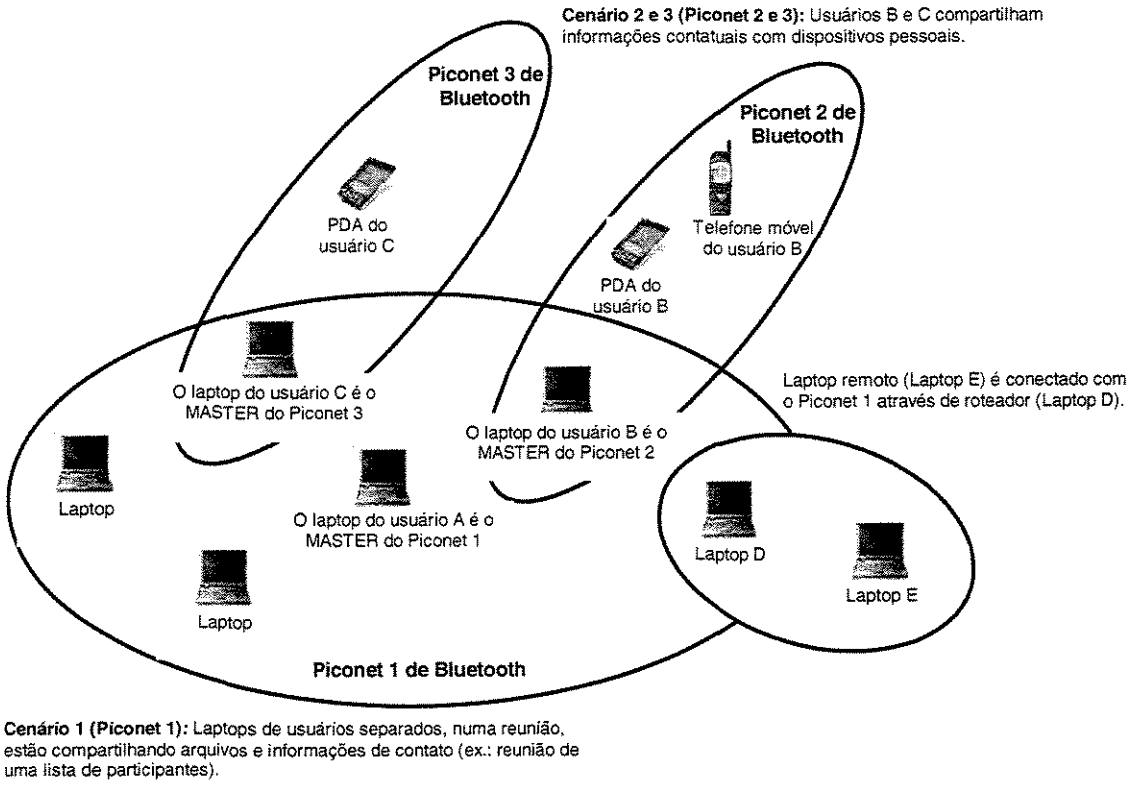


Figura 33 - Uma Rede Bluetooth Típica – Um Scatternet

Roteadores móveis, numa rede *Bluetooth*, controlam as topologias variáveis dessas redes e também o fluxo de dados entre dispositivos que são capazes de suportar uma ligação direta um com outro. Como os dispositivos modificam-se de uma maneira aleatória, as redes devem ser rapidamente reconfiguradas para controlar a topologia dinâmica.

Redes *Bluetooth* podem apoiar qualquer canal de dados assíncrono com até três canais simultâneos de fala síncronos ou um canal que transfere dados assíncronos e fala síncrona, simultaneamente.

Bluetooth usa uma combinação das tecnologias de redes de pacotes e circuitos. A vantagem em usar tecnologias de redes de comutação de circuitos é permitir o roteamento de pacotes múltiplos de informação pelo mesmo caminho de dados. Considerando que este método não consome todos os recursos em um caminho de dados, fica mais fácil os dispositivos remotos manterem dados fluindo ao longo de um *scatternet*.

6.1.1 Arquitetura

Como no padrão IEEE 802.11, *Bluetooth* permite que os dispositivos estabeleçam redes P2P (*Peer to Peer*) ou redes baseadas em pontos de acesso fixos com quem os nós móveis podem se comunicar. Na topologia ad hoc, é fácil interconectar os dispositivos móveis que estão na mesma área. Nesta arquitetura, as estações cliente são agrupadas em uma única área geográfica e podem ser inter-relacionadas sem acesso à rede cabeada (infra-estrutura de rede). A topologia básica do *Bluetooth* é descrita na Figura 33. Como mostrado neste *piconet*, um dos dispositivos seria um mestre e os outros dois dispositivos seriam os escravos.

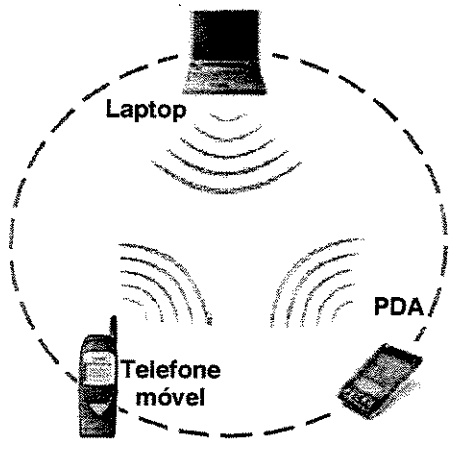


Figura 34 - Topologia Ad Hoc Bluetooth

Ao contrário de uma WLAN, que inclui uma estação sem fios e um ponto de acesso, com *Bluetooth*, existem somente estações sem fios ou clientes.

O *Bluetooth* provê uma de três classes de administração de potência: dispositivos Classe 3 operam a 1 milliwatt (mW) e têm uma distância operacional de 0.1 metro a 10 metros (m); dispositivos Classe 2 operam a 10mW e possuem distância operacional de 10m e os Classe 1 operam à 100mW e têm distância operacional de até 100m.

A distância mais curta pode ser favorável a aplicações como a reposição de cabos (por exemplo, *mouse* ou teclado) e sincronização de arquivos. As distâncias de alta-potência podem alcançar distâncias de 100m. Com essa distância relativamente longa, o *Bluetooth* pode competir com outras tecnologias e aplicações de WLAN.

6.1.2 Benefícios

O *Bluetooth* oferece alguns benefícios aos usuários, que o torna muito atrativo nos dias atuais e pode resultar em aumento de eficiência e redução de custos:

Substituição de Cabos: a tecnologia *Bluetooth* substitui cabos para uma variedade de interconexões. Ela inclui dispositivos periféricos (conexões de mouse e teclado), USB – de 12Mbps (USB 1.1) até 480Mbps (USB 2.0); impressoras e modem, normalmente a 4Mbps; e *headsets* e microfones sem fio que se conectam com PCs ou telefones móveis.

Facilidade de Compartilhamento de Arquivos: *Bluetooth* habilita o compartilhamento de arquivos entre dispositivos com *Bluetooth* habilitado. Por exemplo, participantes de uma reunião com laptop com compatibilidade de *Bluetooth* podem compartilhar arquivos entre si.

Sincronização Sem Fios: *Bluetooth* provê sincronização sem fio automática com outros dispositivos que tenham o *Bluetooth* habilitado. Por exemplo, podem ser sincronizadas informações pessoais contidas em livros de endereço e livros de dados entre PDAs, laptop, telefones móveis e outros dispositivos. A sincronização ocorre automaticamente sempre que os dispositivos estão dentro da distância de transmissão de outro dispositivo, sem o conhecimento do usuário desse dispositivo.

Aplicações Sem Fios Automáticas: o *Bluetooth* suporta funções de aplicação sem fio automáticas. Ao contrário das sincronizações, que tipicamente ocorrem no local, as aplicações automáticas sem fios se conectam com a rede e a Internet.

Conectividade de Internet: o *Bluetooth* é suportado por uma variedade de dispositivos e aplicações. A conectividade de Internet é possível quando os dispositivos e tecnologias se unem para utilizar as capacidades uns dos outros.

6.1.3 Segurança

A segurança do *Bluetooth* é fornecida nas várias ligações sem fios – somente nos caminhos de rádio, como é visto na Figura 34. As ligações de encriptação e autenticação podem ocorrer, mas a verdadeira segurança fim-a-fim não é possível.

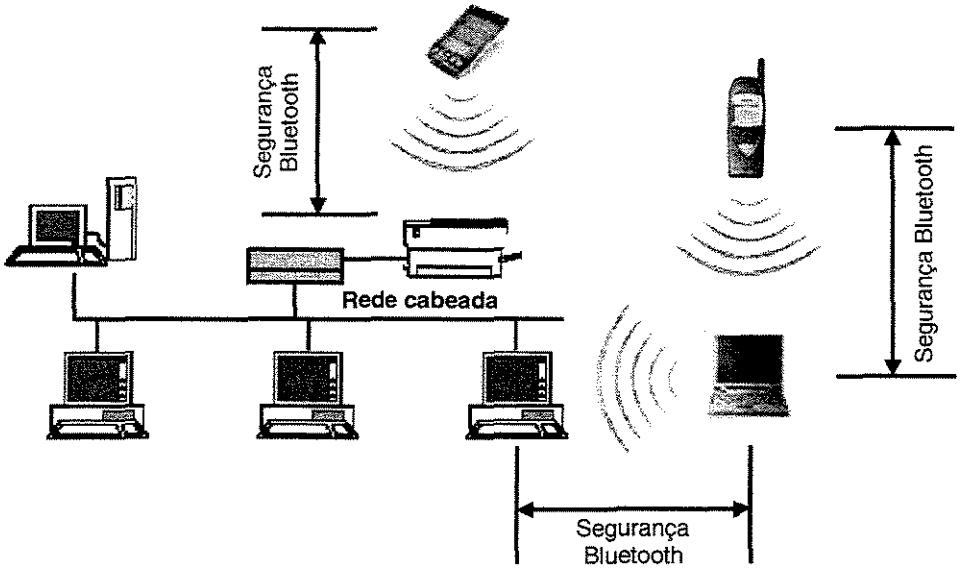


Figura 35 - Interface de Segurança do Bluetooth

Os três serviços de seguranças definidos pelas especificações do *Bluetooth* são [KARYGIANNIS+2002]:

Privacidade: a privacidade é uma das metas de segurança do *Bluetooth*; a intenção é prevenir que a informação seja visualizada (ataque passivo).

Autenticação: a autenticação é a verificação da identidade dos dispositivos de comunicação. Ela evita o recebimento de mensagens de origem duvidosa e acessos não desejados a dados.

Autorização: autorização é o serviço de segurança desenvolvido para permitir o controle de recursos.

Como no padrão 802.11, o *Bluetooth* não possui outros serviços de segurança como a auditoria e o não-repúdio. Se esses serviços são desejados ou requisitados, eles devem ser providos por outros meios.

A arquitetura de segurança *Bluetooth* [MILLER1999], [TRÄSKBÄCK2001], como é vista na Figura 35, é construída no topo das características de segurança do nível de ligação no sistema *Bluetooth*.

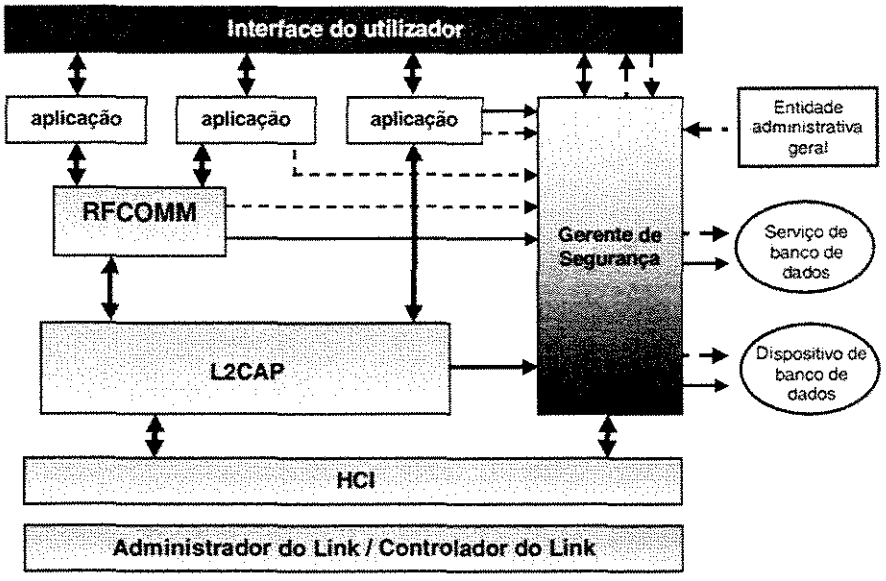


Figura 36 - Arquitetura de Segurança *Bluetooth*

O componente fundamental da arquitetura de segurança *Bluetooth* é o gerente de segurança, responsável pelas seguintes tarefas [VINES2002]:

- Armazenamento de informação segura relacionado com serviços e dispositivo;
- Implementação ou aplicação de protocolo para responder aos acessos requeridos (quer o acesso seja garantido ou recusado);
- Obrigação de autenticação e/ou encriptação antes da conexão na aplicação;
- Inicialização ou processamento de entrada de uma ESCE (*External Security Control Entity*) - dispositivo do utilizador, para definir relações de confiança ao nível de dispositivo;
- Inicialização do emparelhamento e consulta da entrada do PIN pelo utilizador. A entrada do PIN também poderá ser feita por alguma aplicação.

Durante o estabelecimento da conexão, o gerente de segurança *Bluetooth* é requerido e este concede acesso baseado no nível de confiança do dispositivo e no nível de segurança do serviço. Ambos os níveis são levados para bancos de dados internos. Um gerente de segurança centralizado permite fácil implementação de políticas de acesso flexíveis porque as interfaces para protocolos e outras entidades são mantidas simples e limitadas à consulta, resposta e procedimentos de registro.

As políticas de controle de acesso são encapsuladas no gerente de segurança, de

forma que a implementação de políticas mais complexas não afeta a implementação de outras. As implementações podem determinar se a tarefa de inscrição é executada pela própria aplicação ou por uma entidade de administração geral responsável por fixar o caminho da pilha de protocolos e/ou registrar o serviço no momento de sua descoberta.

O gerente de segurança mantém informações seguras para os serviços, em banco de dados seguros, e as aplicações precisam se registrar com o gerente de segurança antes de se tornarem acessíveis.

A característica do *Bluetooth* de operar num esquema de saltos de freqüência de 1,600 hops/segundos, combinada com controle de potência do link de rádio (para limitar a distância de transmissão), dificulta, para um adversário, localizar uma transmissão de *Bluetooth*, e proporciona, conseqüentemente, o aumento da proteção contra o espião e os acessos maliciosos.

O *Bluetooth* apresenta três modos de segurança e, em cada momento, cada dispositivo *Bluetooth* só pode operar num dos modos [ANAND2001], [SWAMINATHA+2002]:

Modo 1 de Segurança: Nenhuma segurança. O dispositivo não inicia nenhum procedimento de segurança automaticamente. Dados sem importância vital são facilmente acessados.

Modo 2 de Segurança: Segurança forçada ao nível de serviço. O dispositivo não inicia procedimento de segurança automaticamente antes da camada L2CAP[7] (*Logical Link Control and Adaptation Protocol*) estabelecer um canal. Estas instalações niveladas aliviam a interação com aplicações que variaram os requisitos de segurança.

Modo 3 de Segurança: Segurança forçada ao nível de ligação. O dispositivo inicia procedimentos de segurança antes que a ligação seja estabelecida. O modo suporta autenticação (unidirecional ou mútua) e encriptação. Estas características estão baseadas numa chave de ligação secreta que é compartilhada por um par de dispositivos e, para gerar a chave, um procedimento emparelhado é usado quando os dois dispositivos se comunicarem pela primeira vez.

Os três modos de segurança do *Bluetooth* são visualizados na Figura 36:

[7] A camada L2CAP forma a interface entre o padrão de protocolos de transporte de dados e o protocolo *Bluetooth*, e provê serviços de dados orientados e não-orientados à conexão através da multiplexação de protocolos, segmentação e remontagem.

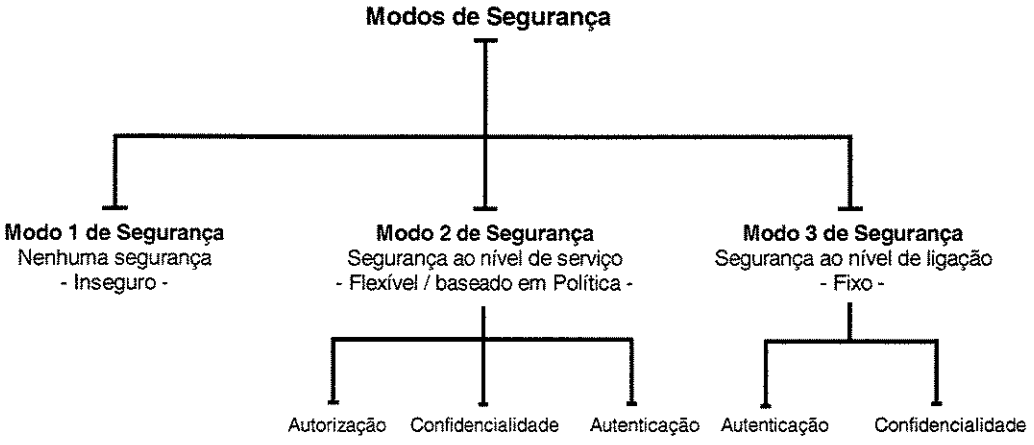


Figura 37 - Taxonomia dos Modos de Segurança Bluetooth

6.1.3.1 Autenticação

O procedimento de autenticação *Bluetooth* é caracterizado pelo esquema de "desafio-resposta". Dois dispositivos interagindo em um procedimento de autenticação são referenciados como pretendente e verificador. O verificador é o dispositivo de *Bluetooth* que valida a identidade de outro dispositivo e o pretendente é o dispositivo que tenta provar sua identidade. O protocolo desafio-resposta valida os dispositivos através da verificação do conhecimento de uma chave secreta – uma chave de ligação *Bluetooth*.

Basicamente, o protocolo verifica se ambos os dispositivos têm a mesma chave, e se sim, faz a autenticação com sucesso. Também, durante o processo de autenticação, um valor ACO (*Authenticated Ciphering Offset*) é gerado e armazenado em ambos os dispositivos. Este valor é usado para gerar, mais tarde, a chave de encriptação.

Na Figura 37, que exemplifica o esquema de verificação de desafio-resposta, um dispositivo *Bluetooth* (pretendente) tenta alcançar e se conectar ao outro (verificador).

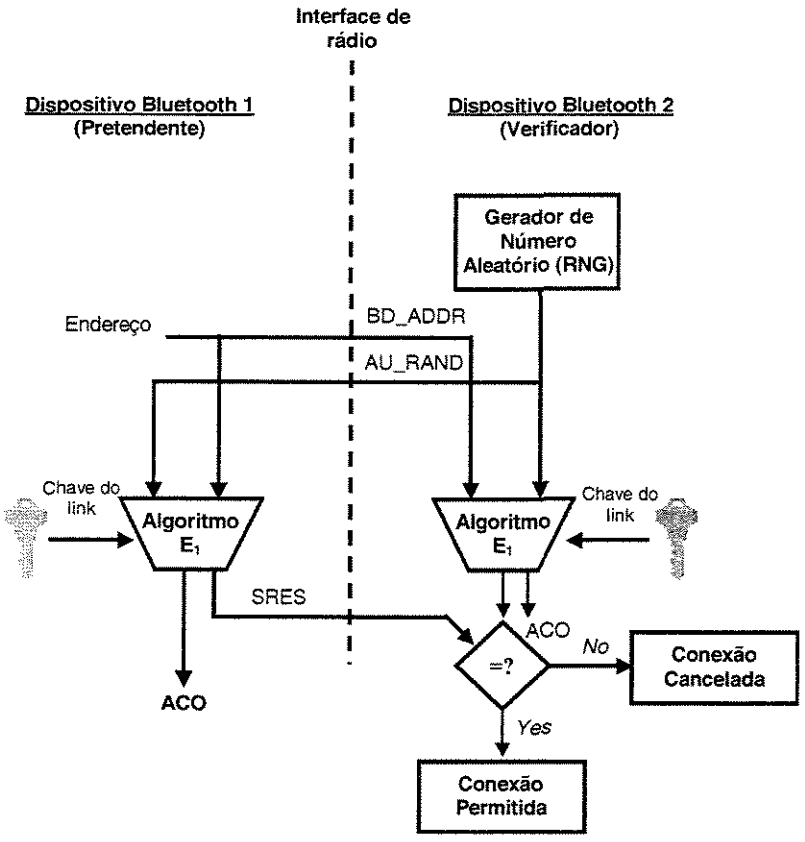


Figura 38 - Autenticação Bluetooth

Os passos do processo de autenticação são os seguintes:

Passo 1: O pretendente transmite seu endereço de 48 *bits* (BD_ADDR) para o verificador. A chave BD_ADDR é única para cada dispositivo *Bluetooth*.

Passo 2: O verificador transmite um desafio aleatório de 128 *bits* (AU_RAND) para o pretendente. O AU_RAND pode ser derivado de um processo aleatório ou *pseudo-random* dentro do dispositivo *Bluetooth*. Ele não é um parâmetro estático, podendo mudar freqüentemente.

Passo 3: O verificador, através do algoritmo E1, computa uma resposta de autenticação utilizando o endereço, a chave de ligação e o desafio aleatório como entradas. O pretendente executa a mesma computação.

Passo 4: O pretendente devolve a resposta computada (SRES – *Signed Response*) ao verificador.

Passo 5: O verificador compara o SRES do pretendente com o seu SRES.

Passo 6: Se os dois valores de SRES de 32 *bits* forem iguais, o verificador continuará o estabelecimento da conexão.

Esta aplicação indica que vai ser autenticado. Aqui, repara-se que o verificador não tem a obrigatoriedade de ser o mestre, pois algumas das aplicações apenas requerem uma via de autenticação (apenas uma parte é autenticada), e não a autenticação mútua.

Caso ocorram falhas na autenticação, um dispositivo *Bluetooth* deverá esperar um intervalo de tempo antes de realizar uma nova tentativa. Este intervalo de tempo sofrerá aumentos exponenciais para prevenir que adversários tentem ganhar acesso derrotando o esquema de autenticação através de tentativas e erros, com diferentes chaves.

O padrão *Bluetooth* permite a execução das autenticações unidirecional e mútua e, para a validação, se baseia nos algoritmos SAFER (*Secure And Fast Encryption Routine*) .

O endereço de *Bluetooth* é um parâmetro público e único para cada dispositivo e pode ser obtido através de um processo de investigação do dispositivo. A chave de ligação, ou chave privada, é uma entidade secreta derivada durante a inicialização e nunca é descoberta fora do dispositivo *Bluetooth* nem é transmitida em cima da interface aérea. O desafio aleatório, designado para ser diferente em toda transação, e a resposta criptográfica (SRES) também são parâmetros públicos de autenticação. Com o conhecimento do desafio e dos parâmetros de resposta, deveria ser impossível predizer o próximo desafio ou derivar a chave de ligação.

6.1.3.2 Confidencialidade

Bluetooth provê um serviço de segurança de confidencialidade para obstruir as tentativas dos invasores na interface aérea. O procedimento de encriptação, utilizado para proteger o *payload* de cada pacote trocado entre dois dispositivos *Bluetooth*, se baseia na cifra corrente E_0, que é ressincronizada para cada *payload*.

De acordo com a Figura 38, o algoritmo criptográfico gera uma seqüência de *bits* pseudo-aleatório (*Keystream*), através do LFSR (*Linear Feedback Shift Registers*) do gerador da chave corrente. As entradas da função criptográfica são o identificador mestre (BD_ADDR), um número aleatório (EN_RAND), um número de *slot* e a chave de encriptação, que inicializa os LFSRs antes da transmissão de cada pacote.

A chave criptografada, fornecida pelo algoritmo de encriptação, é produzida usando um gerador de chave (KG) interno, e este dá origem a chave de cifra corrente, a um número aleatório (EN_RAND novamente) e ao valor ACO. O parâmetro ACO é outro parâmetro de saída do processo de autenticação.

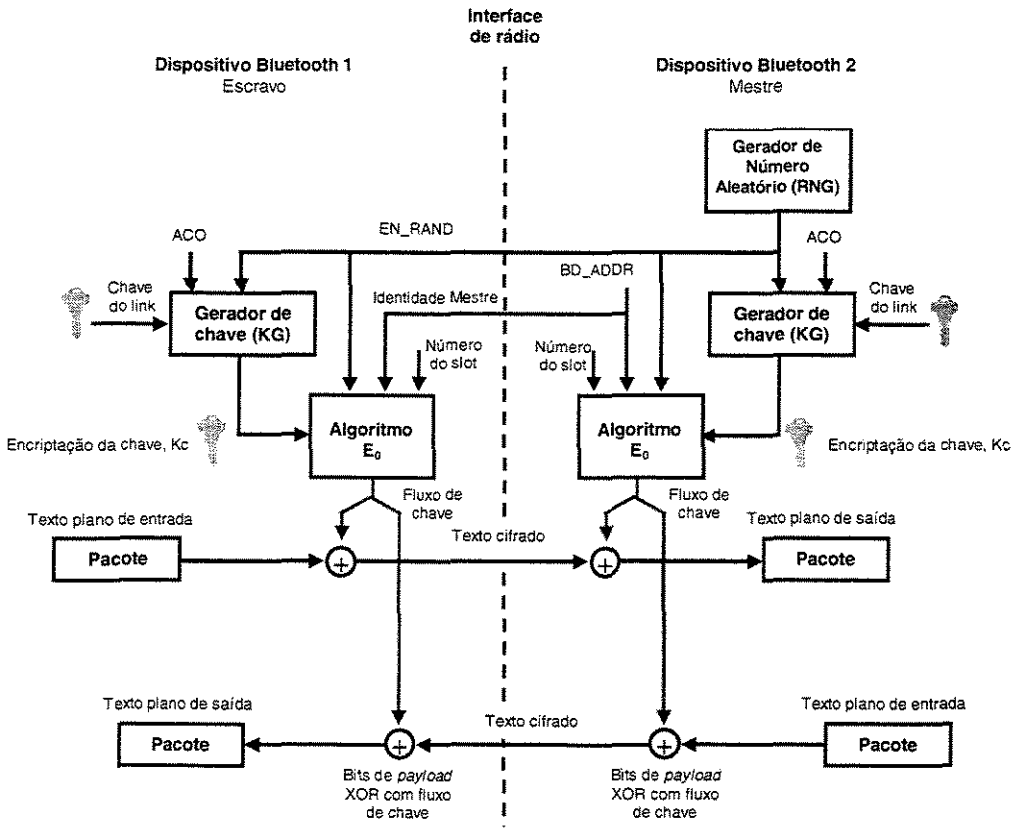


Figura 39 - Procedimento de Encriptação do Bluetooth

O tamanho da chave criptografada Kc varia de 8 a 128 *bits* e pode ser negociado entre os dispositivos mestre e escravo. Durante a negociação, o dispositivo mestre oferece uma sugestão de tamanho de chave ao escravo. Em toda aplicação, um parâmetro "mínimo aceitável" de tamanho de chave pode ser fixado para prevenir que usuários maliciosos estabeleçam o tamanho mínimo de 8 *bits* para a chave - tornando a ligação totalmente insegura.

Os três modos de encriptação suportados por *Bluetooth* são os seguintes [KARYGIANNIS+2002]:

Modo 1 de encriptação: Nenhuma encriptação é realizada em nenhum tráfego.

Modo 2 de encriptação: O tráfego *broadcast* (ponto-multiponto) fica desprotegido (não encriptado), mas o tráfego endereçado individualmente é criptografado com a chave mestre.

Modo 3 de encriptação: Todo o tráfego é criptografado com a chave mestre.

Pela especificação do *Bluetooth*, dois dispositivos associados simultaneamente

derivam chaves de ligação na fase de inicialização, quando um usuário entrar com um PIN idêntico em ambos os dispositivos, conforme a Figura 39. Depois de completada a inicialização, os dispositivos, automática e transparentemente, autenticam e executam a encriptação da ligação. O código PIN pode variar entre 1 e 16 bytes; um típico PIN de 4 dígitos pode ser suficiente para algumas aplicações; porém, códigos mais longos também podem ser necessários.

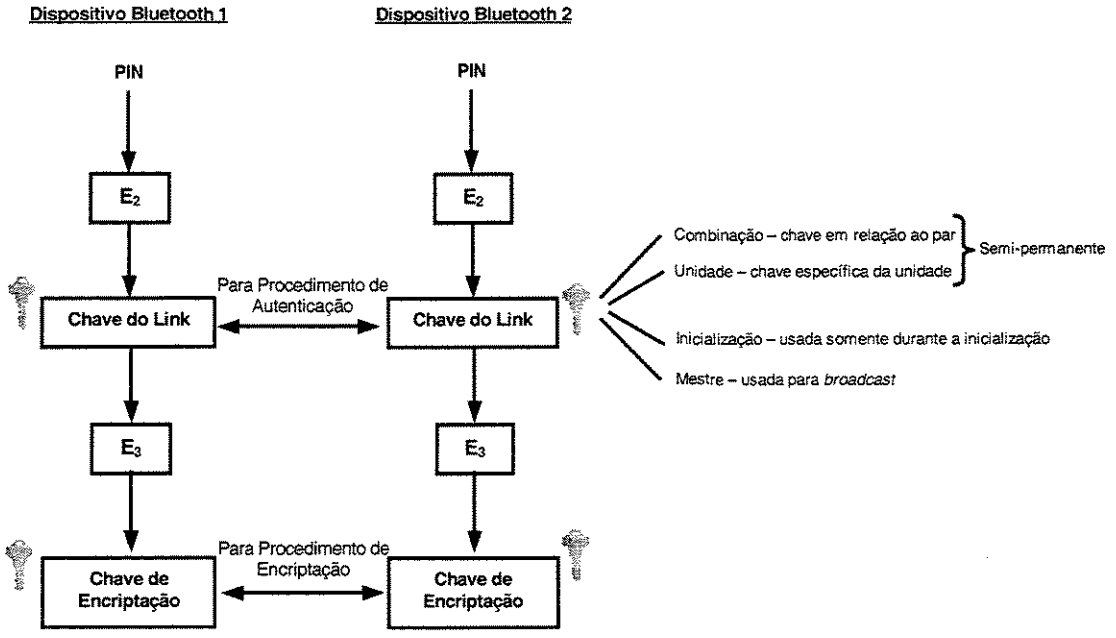


Figura 40 - Geração de Chave *Bluetooth* de PIN

6.1.3.3 Níveis de Confiança, de Serviço e Autorização

Além dos modos de segurança, a tecnologia *Bluetooth* permite níveis de confiança e níveis de segurança de serviço. Os dois níveis de confiança são: "confiado" e "não confiado". Dispositivos "confiados" são aqueles que têm relacionamento fixo e acesso completo a todos os serviços. O dispositivo foi previamente autenticado, uma chave de ligação é guardada e o dispositivo é marcado como "de confiança" na base de dados do dispositivo.

Os dispositivos "não confiados", por não manterem relacionamento permanente, têm acesso restrito aos serviços. O dispositivo foi previamente autenticado, uma chave de ligação é guardada, mas o dispositivo não é marcado como "de confiança" na base de dados do dispositivo. A tabela de base de dados do dispositivo é uma entidade mantida pelo gerente de segurança.

Para os serviços, três níveis de segurança são definidos [KARYGIANNIS+2002]:

Nível de serviço 1: requer autorização e autenticação; só é concedido acesso automático aos dispositivos "confiados", e os "não confiados" necessitam de autenticação manual.

Nível de serviço 2: requer somente autenticação. O acesso à aplicação é permitido somente após o procedimento de autenticação, e a autorização não é necessária.

Nível de serviço 3: todos os dispositivos são expostos. A autenticação não é requerida e o acesso é concedido automaticamente.

Toda informação a respeito dos níveis de segurança de um serviço também é guardada na base de dados de serviço do gerente de segurança.

Associados a esses níveis, estão os controles de segurança para restringir acessos aos serviços: autorização requerida (isso sempre inclui autenticação) e autenticação requerida e encriptação requerida (a ligação deve ser codificada antes que a aplicação possa ser acessada).

6.1.4 Problemas de Segurança com o padrão *Bluetooth*

A tecnologia *Bluetooth*, apesar de possuir medidas de segurança bastante consistentes, apresenta algumas vulnerabilidades preocupantes [VAINIO2000]:

- A força do gerador pseudo-randômico do desafio-resposta não é conhecida: O Gerador de Número Randômico (RNG – *Random Number Generator*) pode produzir número estático ou números periódicos que podem reduzir a efetividade do esquema de autenticação.
- Os códigos PINs possuem, tipicamente, somente 4 dígitos: Os PINs, que são usados para a geração das chaves de ligação e encriptação, podem ser adivinhados facilmente. Aumentando o tamanho do PIN, em geral, aumenta-se a segurança.
- Não existe um modo elegante para gerar e distribuir os PINs: O estabelecimento dos PINs em grandes redes *Bluetooth* com muitos usuários pode ser difícil. Problemas de escalabilidade, freqüentemente, acarretam problemas de segurança, e os PINs sofrem todos os problemas típicos das senhas, como não ser alterado, ser esquecido, ser compartilhado, etc.

- A chave de inicialização pode ser muito fraca: É necessário o desenvolvimento de um procedimento de geração da chave de inicialização mais robusto.
- A chave do dispositivo é reutilizada e por isso, torna-se pública: A chave do dispositivo deve ser usada como entrada para gerar a chave aleatória e, ao invés de utilizar somente uma chave do dispositivo, um jogo de chaves é preferível.
- A chave mestre é compartilhada: É necessário o desenvolvimento de um esquema de dispersão de chaves melhor.
- Não existe nenhuma autenticação do usuário: É notada somente a autenticação do dispositivo. A segurança no nível de aplicação e a autenticação de usuário podem ser empregadas.
- Tentativas repetitivas para a autenticação: É preciso desenvolver uma característica limite para prevenir os pedidos ilimitados.
- O algoritmo de fluxo de cifra E_0 é considerado fraco: Um procedimento de encriptação mais robusto é requerido.
- Tamanho da chave negociável: Deve ser feito um acordo global para a determinação de um tamanho mínimo de chave.
- As espionagens resultam no compartilhamento da chave do dispositivo: Um usuário corrupto pode ser capaz de comprometer a segurança (obtendo acesso sem autorização) entre dois outros usuários se conseguir estabelecer comunicação com qualquer um dos dois. Isso ocorre porque a chave de ligação (chave do dispositivo), derivada da informação compartilhada, é descoberta.
- A privacidade pode ser comprometida se o endereço do dispositivo *Bluetooth* (BD_ADDR) for capturado e associado com um usuário particular: Uma vez que o BD_ADDR é associado a um usuário particular, suas atividades podem ser registradas, ocasionando a perda de privacidade.
- A autenticação do dispositivo é baseada num simples mecanismo de desafio-resposta de chave compartilhada. A autenticação mútua é exigida para verificar se os usuários e a rede são legítimos.
- A segurança fim-a-fim não é implementada: Somente ligações individuais são encriptadas e autenticadas. Os dados são decifrados em pontos intermediários. Devem ser desenvolvidos *softwares* de aplicação sobre o *software* de *Bluetooth*.
- Os serviços de segurança são limitados: A auditoria, o não-repúdio e outros serviços não existem; se forem necessários, eles podem ser implementados em pontos particulares da rede *Bluetooth*.

6.1.5 Contra-Medidas de Segurança para o padrão *Bluetooth*

O *Bluetooth* ainda é um padrão relativamente novo; porém, contra-medidas estão disponíveis para auxiliar na segurança dessas redes.

Algumas contra-medidas utilizadas, consideradas como técnicas, envolvem duas categorias: soluções de software e hardware. As soluções de software focalizam o PIN e as autenticações privadas, enquanto que as soluções de hardware envolvem o uso do endereço do dispositivo *Bluetooth* e as chaves de ligação que residem no nível de ligação.

6.1.5.1 Soluções de *Software*

Bluetooth exige códigos PIN no nível de ligação. O tamanho dos PINs poderia variar de 1 a 16 octetos (8 *bits* a 128 *bits*), dependendo do grau de segurança selecionado pelo usuário do dispositivo. Os dispositivos *Bluetooth* usam códigos PINs, efetivamente, para a autenticação do dispositivo: o PIN age como uma variável no processo de geração da chave de inicialização. Para a autenticação entre dois dispositivos, o *Bluetooth* tem a opção de armazenar e restaurar os códigos automaticamente e diretamente da memória, ou obter o código PIN de usuário no dispositivo quando este for inicializado. Pelo fato dos códigos PINs serem necessários para a autenticação e para o nível de ligação, os administradores deveriam assegurar que os dispositivos *Bluetooth* usariam códigos diferentes dos *default* (0000).

O dispositivo *Bluetooth* deveria empregar a autenticação do dispositivo como uma camada extra de segurança; poderia ser incorporando um software em nível de aplicação que exigisse senha de autenticação para segurança. Novamente, as senhas são medidas fundamentais e adicionam mais uma etapa de segurança.

6.1.5.2 Soluções de *Hardware*

Como já mencionado, a camada de ligação provê sua própria forma de segurança. O *Bluetooth* utiliza um endereço de dispositivo único para cada um deles; esse endereço, um identificador de 48 *bits*, serve para vários propósitos, como gerar chaves de ligação de 128 *bits* e chaves de encriptação. Por exemplo, o algoritmo de geração de chaves (definido pelo padrão *Bluetooth*), em combinação com um número aleatório gerado e o endereço do

dispositivo *Bluetooth*, cria as chaves de unidade e combinação.

As chaves de ligação, números randômicos de 128 *bits* que formam a base da segurança *Bluetooth*, estão na forma da chave de unidade, da chave mestre temporária e das chaves de combinação e inicialização. O dispositivo na rede gera a chave de unidade (uma chave raramente alterada) quando um novo dispositivo entra primeiro em operação, e então, a chave da unidade pode se tornar a chave de ligação do dispositivo para a rede. Porém, já que o compartilhamento de chaves de ligação representa uma vulnerabilidade, as organizações deveriam regular a troca de chaves de unidade com dispositivos não-confiáveis.

As chaves de combinação são derivadas da comunicação entre dois dispositivos e se tornam uma chave de ligação única somente para esses dois dispositivos. Isso adiciona uma camada de segurança porque requer que um usuário malicioso possua ambas as chaves de unidade, ao invés de uma só. É importante saber que a chave de unidade e as chaves de combinação são, funcionalmente, indistinguíveis; a diferença está na maneira como elas são geradas. Conseqüentemente, um dispositivo *Bluetooth* pode possuir uma chave de unidade ou uma chave de combinação, mas não ambas.

Uma outra solução de hardware considerada pode ser o uso de esquemas de saltos de freqüência, que permitem que dispositivos se comuniquem até mesmo em áreas onde há muita interferência eletromagnética. Os esquemas de saltos de freqüência também oferecem proteção contra erros de estouro causados pelo contínuo movimento dos sinais dentro e fora da faixa de interferência e permitem a correção desses erros usando FEC (*Forward Error Correction*). Outro benefício dos esquemas é proteger os usuários autorizados dos maliciosos, através da transmissão de sinais com uma seqüência pseudo-randômica que move o sinal arbitrariamente ao redor da banda larga; isso faz com que o sinal seja dificilmente localizado. Essa técnica fornece uma proteção mínima, mas não deve ser considerada a única fonte de confiança.

A biometria, mais especificamente a autenticação de voz, também poderia ser utilizada para oferecer segurança aos dispositivos da rede. A autenticação de voz pode ajudar as organizações a prevenir que usuários maliciosos comprometam os dispositivos *Bluetooth* remotos e as redes.

A tecnologia *Bluetooth* não foi projetada, originalmente, para transmissões de dados verdadeiramente sensíveis. O *Bluetooth* não é um concorrente do WLAN; ele foi desenhado para formar PANs, onde a segurança é conveniente, mas não essencial.

Como algumas vulnerabilidades já foram detectadas, é provável que o padrão continue evoluindo e os mecanismos de segurança de hardware embutidos nos dispositivos se tornem cada vez mais robustos.

Antes do ano de 2007, quando é esperado que o *Bluetooth* esteja totalmente maduro e seja uma das tecnologias de redes sem fios onipresentes, a segurança deverá ter melhorado, no sentido de minimizar os riscos de seu desenvolvimento.

Capítulo 7

Comparativo dos aspectos de segurança de outras tecnologias de redes sem fios existentes

Além das tecnologias de redes sem fios já citadas no trabalho, existem outras no mercado que merecem destaque:

7.1 Outros Padrões para WWAN: GPRS e UMTS

O sistema GSM, dentre os sistemas móveis de 2ª geração, é o mais utilizado, pois o seu desenvolvimento envolveu o maior número de inovações em comparação a todos os padrões da referida geração. Estas inovações redundaram em um padrão que vem permitindo uma fácil evolução do sistema GSM nas suas várias fases, incluindo o GPRS, que permite a transmissão de dados usando comutação de pacotes. Isso serviu de base para a proposição do sistema de 3ª geração UMTS.

Apresentaremos, a seguir, algumas características dos sistemas GPRS e UMTS e os seus principais aspectos de segurança.

7.1.1 Segurança nos Sistemas GPRS

A tecnologia GPRS foi publicada em 1997, pelo ETSI e surgiu como forma de suportar os serviços de dados, pois foram criadas baseadas em transmissão por comutação de pacotes, diferentemente da tecnologia GSM [WATKINS2000].

Os sistemas GSM e GPRS possuem características em comum, como as bandas de freqüência, estrutura de *frames,* técnicas de modulação e interface aérea, pois em GPRS, é utilizada uma combinação de FDMA e TDMA.

A rede GPRS pode ser considerada como um acréscimo à rede GSM, com tráfego orientado a pacotes mediante algumas modificações na arquitetura.

A arquitetura do sistema GPRS é composta por [WATKINS2000]:

- SGSN (*Serving GPRS Support Node*) – responsável pela entrega dos pacotes de dados que possuem as estações móveis como origem e destino e pelas funções de autenticação, roteamento, gerenciamento de mobilidade e controle de acesso.
- GGSN (*Gateway GPRS Support Node*) – responsável pela gerência do roteamento entre a rede GPRS e outras redes de dados.
- HLR (*Home Location Register*) – possui a mesma função do HLR para as redes GSM, e também armazena o endereço do protocolo de pacote de dados (PDP) para cada usuário.
- LR (*Location Register*) – contém a localização corrente e o perfil de usuário para todos os usuários da área de serviço; é similar ao LR do GSM.

No que diz respeito à segurança, as redes GPRS também suportam os aspectos de autenticação da identidade do usuário, confidencialidade da informação do usuário e da identidade do assinante [BROOKSON2001].

Autenticação do Assinante

Nas redes GPRS, o procedimento de identificação e autenticação do assinante é idêntico ao das redes GSM, ou seja, o usuário é identificado pelo próprio processo de identificação, tendo como base os dados presentes no módulo SIM do MS. É a partir deste processo de autenticação que é determinada a chave criptográfica de seção a ser utilizada.

Um novo usuário cadastrado na rede recebe da operadora uma chave de autenticação K_i (128 *bits*) e sua identificação IMSI, as quais são gravadas no seu módulo SIM e também no centro de autenticação AUC.

A autenticação da MS é feita através da requisição, pelo conjunto BSS/MSC/VLR, das informações de segurança dos usuários, armazenadas nos vetores RAND e SRES e fornecidas pelo HLR/AUC. RAND é uma seqüência aleatória de 128 *bits* e o SRES é o resultado da execução do algoritmo de cifragem A3, tendo como entradas RAND e K_i.

O MSC/VLR, ao efetuar a autenticação, escolhe um elemento *j* dentre os elementos do vetor RAND e o envia para o MS; este recebe RAND(*j*) e passa-o para o SIM. O módulo SIM determina o valor SRES(*j*) e o devolve para o MS enviá-lo para o conjunto BSS/MSC/VLR, onde este valor é comparado àquele armazenado e originalmente calculado por HLR/AUC. Se os valores forem iguais, o processo de autenticação teve sucesso. Esse tipo de autenticação é chamado de "desafio-resposta", pois envolve uma chave secreta de autenticação compartilhada por duas entidades.

O processo de autenticação das redes GPRS pode ser visto na Figura 40 [PEREZ+2003].

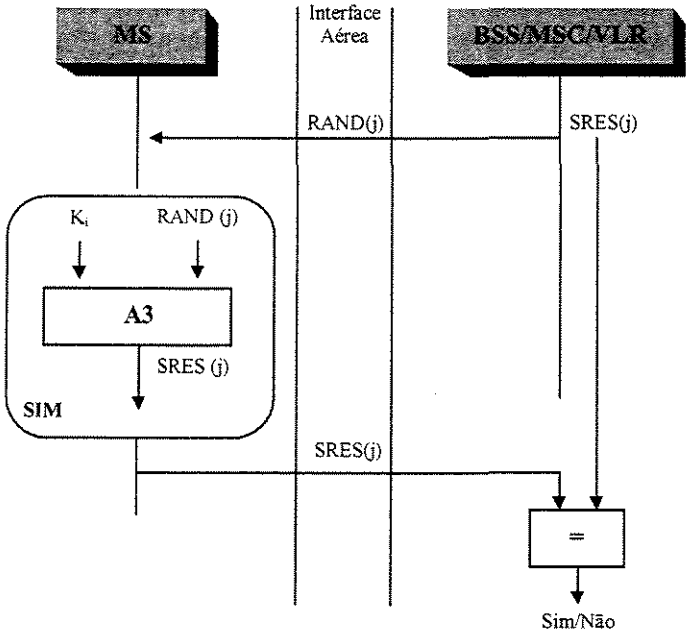


Figura 41 - Processo de Autenticação das Redes GPRS

Confidencialidade dos Dados

Para garantir que nenhum intruso consiga captar a informação transmitida por rádio, o GPRS utiliza o algoritmo criptográfico GPRS/A5 (GPRS *Encryption Algorithm* – GEA). Por ser mais adequado à comutação de pacotes, o ciframento, em GPRS, ocorre na camada superior LLC entre o aparelho MS e a SGSN.

Confidencialidade da Identidade do Assinante

Para preservar a confidencialidade da identificação, o sistema GPRS utiliza os recursos TLLI (*Temporary Logical Link Identify*) e RAI (*Routing Area Identify*) em substituição, respectivamente, ao TMSI e LAI do GSM.

Ambos TLLI e RAI, em GPRS, são tratados pelo SGSN.

7.1.2 Segurança nos Sistemas UMTS

As redes UMTS, consideradas de terceira geração, surgiram da necessidade de aumentar as taxas de transmissão oferecidas pelas redes GPRS. O principal objetivo da

construção da nova tecnologia era especificar e padronizar uma estrutura global de comunicações que permitisse acesso móvel sem fronteiras e de alta velocidade [UMTS1997].

A interface aérea do UMTS é baseada no padrão WCDMA, que possibilita maiores taxas de transmissão, proporcionando espaços para serviços multimídia nas redes celulares e atendendo ao desejo do mercado. Apesar de suportar tráfegos de dados intensos e muitos serviços comuns encontrados nas redes fixas, as redes GPRS não eram capazes de suportar tais serviços.

A arquitetura do sistema UMTS é composta por [LANGNES2001], [WATKINS2000]:

- USIM (*User Subscriber Identify Module*) – semelhante ao SIM do GSM e do GPRS.
- TE (*Terminal Equipment*) – contém a pilha de protocolo no lado do usuário da conexão *wireless*.
- TA (*Terminal Adapter*) – é o software que faz a ligação entre o TE e o terminal móvel (MT).
- MT (*Mobile Terminal*) – é o equipamento utilizado pelo usuário para acessar a rede fixa.
- URAN (*UMTS Radio Access Network*) – contém as estações base para a comunicação com os terminais móveis.
- IWU (*Interworking Units*) – são responsáveis pela adaptação do acesso UMTS às redes principais específicas existentes.
- ICN-IWU (*Intercore Network Interworking Units*) – permite a interoperabilidade entre várias redes do núcleo da terceira geração.

Os sistemas UMTS provêem mecanismos de segurança destinados a fornecer requisitos de confidencialidade, autenticação e disponibilidade.

Autenticação do Assinante

As redes UMTS não possuem padrões definidos para o algoritmo de autenticação; elas utilizam um protocolo de desafio-resposta, realizando autenticação mútua entre o usuário e a rede. Nesse protocolo, a rede de serviço SN (*Service Network*) trabalha com cinco componentes de segurança: um número aleatório (RAND), uma resposta de

autenticação (XRES), uma chave para o ciframento (C_k), uma chave de integridade (I_k) e um token de autenticação (AUTN).

A Figura 41 mostra o processo de autenticação do UMTS [PEREZ+2003].

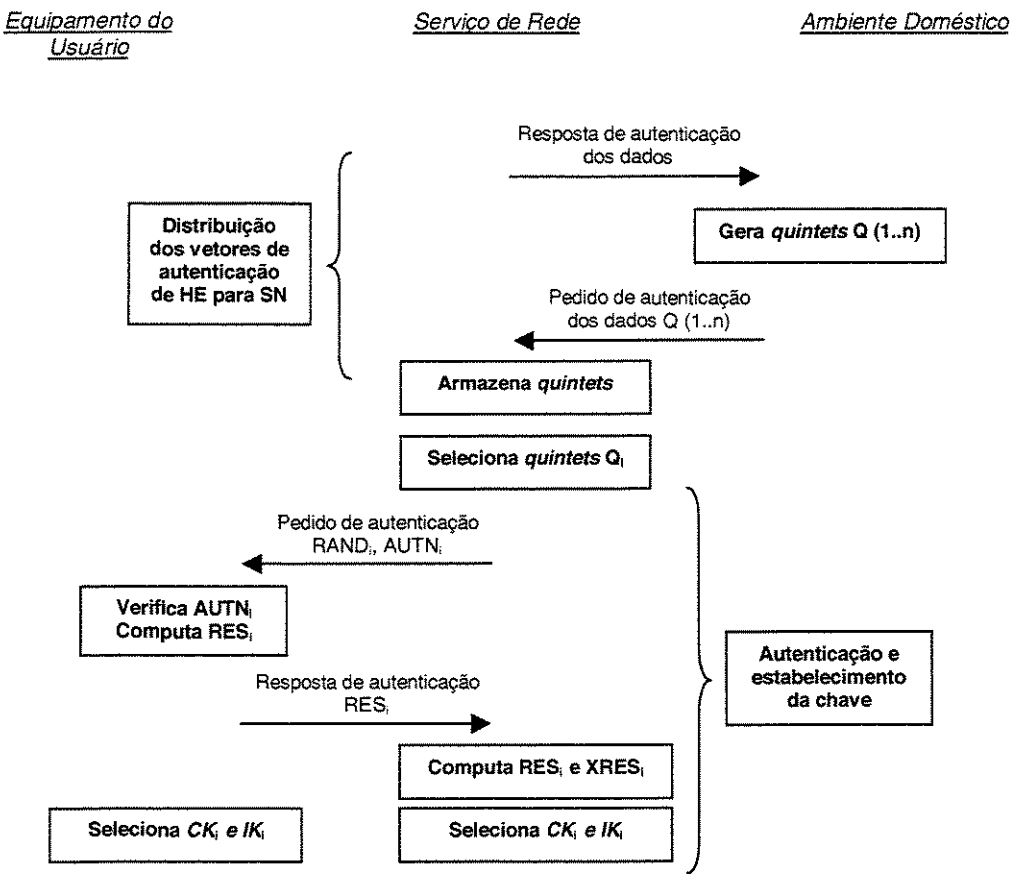


Figura 42 - Processo de Autenticação em Redes UMTS

Confidencialidade dos Dados

O UMTS utiliza, para manter a confidencialidade dos dados, o algoritmo UEA (*UMTS Encryption Algorithm*) não secreto, de modo que sua "força" não está em seu desconhecimento, mas sim na sua própria robustez.

As mensagens transmitidas e recebidas são cifradas através do algoritmo de *stream cipher* f8, baseado no algoritmo KASUMI (algoritmo de cifra por blocos que produz 64 *bits* de saída derivados de 64 *bits* de entrada, controlados por uma chave de 128 *bits*).

O algoritmo f8 recebe cinco parâmetros – CK (*Cipher Key*), uma chave de 128 *bits*; BEARER, identificador de 5 *bits* de *radio bearer* (canal lógico utilizado); DIRECTION,

flag de 1 bit que age como identificador de direção; LENGTH, identificador do tamanho da *keystream* gerada pelo f8 e COUNT-C, número da seqüência de ciframento de 32 *bits* – e gera um bloco de *keystream* que será binariamente adicionado (xor) ao *data stream*. A Figura 42 [PEREZ+2003] apresenta o algoritmo f8.

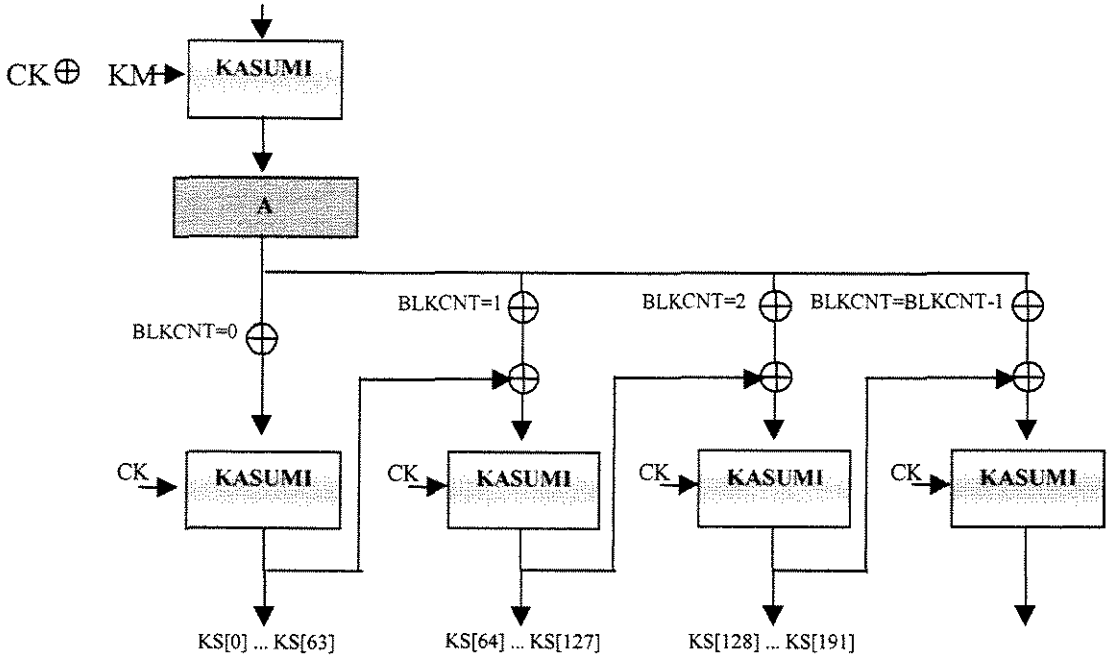


Figura 43 - Algoritmo de Encriptação f8 do UMTS

Confidencialidade da Identidade do Assinante

Este mecanismo permite a identificação do usuário no acesso ao link de rádio através de um *Temporary Mobile Subscriber Identity* (TMSI). Um TMSI tem significado local apenas em um área de localização na qual o usuário é identificado. Fora desta área, ele deve ser acompanhado por um *Location Area Identification* (LAI) ou *Routing Area Identification* (RAI) para evitar ambigüidades. A associação entre a identificação permanente (IMSI) e a temporária (TMSI) do usuário é mantida na VLR/SGSN, na qual o usuário está registrado. A TMSI, quando disponível, é normalmente usada para identificar o usuário no caminho de acesso à rede, para ocorrência de requisições de *paging*, atualização localização, serviços, restabelecimento da conexão, *attachs* e *detachs*.

7.2 Outros Padrões para WLAN: HiperLAN e HomeRF

O crescimento da mobilidade e da flexibilidade foram fatores importantes para a evolução das redes cabeadas para as *wireless* LAN (WLAN). Várias tecnologias de WLAN estão disponíveis no mercado, como 802.11, HiperLAN/2 e HomeRF; cada uma delas com variações de níveis de padronização e interoperabilidade.

Apresentaremos, a seguir, os sistemas HiperLAN (*High Performance Radio LAN*) e Home RF (*Home Radio Frequency*), destacando os requisitos de segurança de autenticação e confidencialidade dos dados.

7.2.1 Segurança nos Sistemas HiperLAN

As redes *HiperLAN* foram especificadas na Europa pela ETSI, a partir de 1992, devido à necessidade de LANs sem fio de alta velocidade. Elas utilizam taxas de sinalização em torno de 23 Mbps, e procuram atingir os mesmos níveis de desempenho do padrão Ethernet.

O padrão original é o *HiperLAN/1* e é considerado uma rede local sem fio que permite mobilidade e suporte a topologias de redes baseadas tanto em infra-estrutura como em redes *ad hoc*. O HiperLAN/1 suporta taxas de 20 Mbps.

Existem outras categorias de *HiperLANs*, que são [VINES2002]:

- *HiperLAN/2* – acesso fixo a redes IP, ATM (*Asynchronous Transfer Mode*) e UMTS para terminais portáteis e móveis limitadamente. Suporta taxas de 24 Mbps.
- *HiperLAN/3* (*HiperAccess*) – acesso local fixo (PMP) a redes IP e ATM, a taxas de até 48 Mbps.
- *HiperLAN/4* (*HiperLink*)– estacionário ponto-a-ponto e taxas de 155 Mbps.

O HiperLAN/2 apresenta uma flexibilidade de uso que vai desde aplicações em escritórios a transmissões multimídias domésticas. Isso é possível por apresentar uma taxa de transmissão que pode chegar a até 54 Mbps aliado ao suporte ao QoS (*Quality of Service*).

A topologia das redes HiperLAN/2 é caracterizada pela comunicação dos terminais móveis (TM) com os pontos de acesso (AP) através da interface aérea definida pelo padrão

HiperLAN/2, ou pela comunicação direta entre dois TMs, conforme a Figura 43 [JOHNSSON1999]. Um usuário de um TM pode se mover livremente pela rede, e um TM, depois de ter feito a associação na rede, se comunica somente com um AP por vez. Os APs da rede vão coletar informações sobre a interface aérea levando em conta as mudanças na topologia desta.

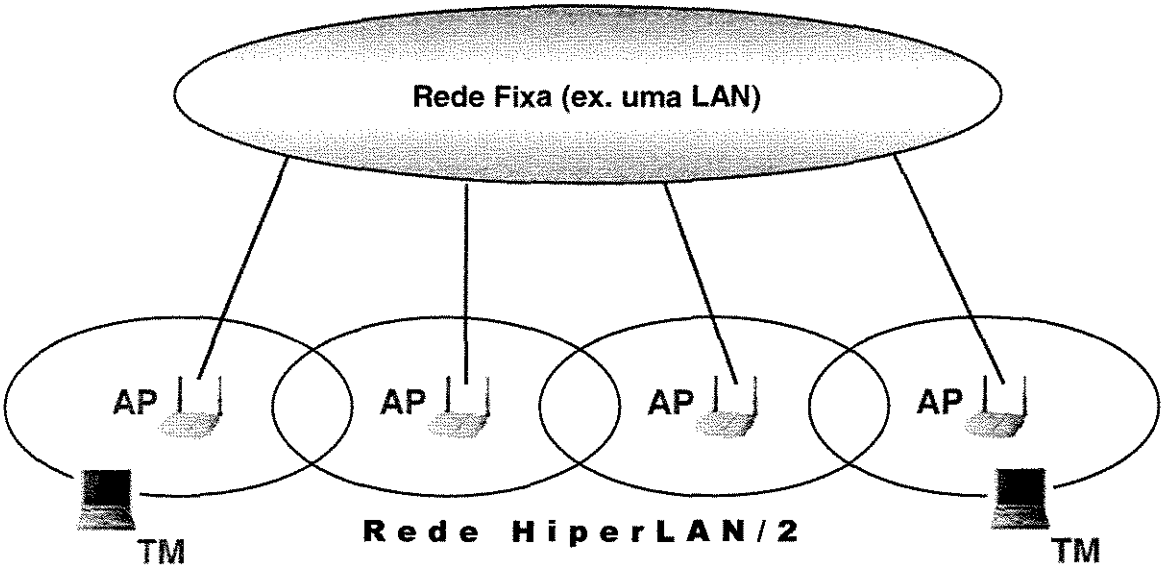


Figura 44 - Topologia Típica das Redes HiperLAN/2

Uma das características da tecnologia HiperLAN/2 é o suporte a segurança, pois nos casos de uso fraudulento e interceptação da transmissão, os sistemas HiperLAN/2 são vulneráveis a ataques.

Os sistemas de rádio, em geral, são sensitíveis às escutas as escondidas e às interceptações das transmissões, porque, nesses sistemas, o sinal carregando a informação não é restrito, por exemplo, ao cabo onde é guiado; ele é espalhado no "ar" e essa distribuição espacial pode ser dificilmente controlada.

Como mecanismos de segurança, o HiperLAN/2 implementa algoritmos de autenticação e criptografia da informação transmitida.

A autenticação é utilizada para que os pontos de acesso garantam que somente os TMs autorizados tenham acesso a rede. Do ponto de vista do terminal, a autenticação assegura que os MTs estarão acessando e trocando informações com as redes seguras.

Os links estabelecidos podem dar suporte ao tráfego de dados criptografados. Isso protege as informações contra interceptação do sinal por um receptor não autorizado. O HiperLAN/2 criptografa os dados pela implementação dos algoritmos DES (*Data Encryption Standard*) ou Triple-DES, que usa uma chave de 56 *bits*.

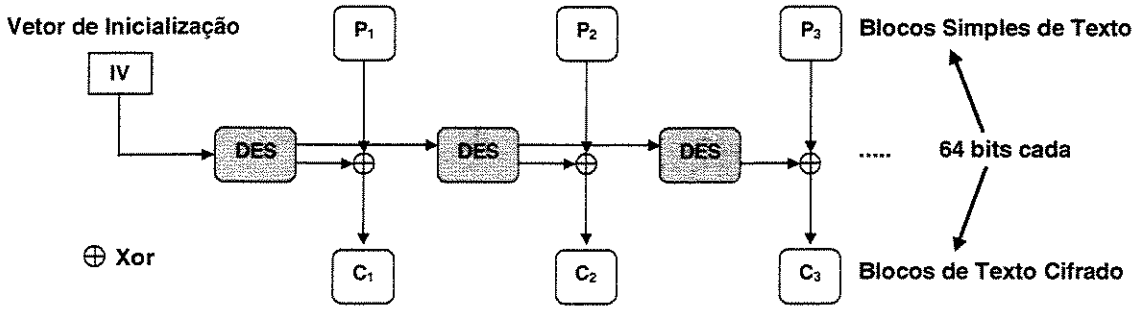


Figura 45 - Algoritmo DES utilizado em HiperLAN/2

Como é visto na Figura 44 [JOBMANN+], o DES opera em modo de produção-realimentação (OFB – *Output-feedback*), que proíbe a propagação de erros de recepção e restringe-os aos *bits* realmente errôneos.

O vetor de inicialização (IV) é encriptado por DES para a construção do primeiro bloco. Uma operação XOR é executada entre a produção de DES e o primeiro bloco simples de texto. Cada um dos blocos tem tamanho de 64 bytes. No segundo passo, a primeira produção de DES é novamente encriptada por DES e XORed com o segundo bloco simples de texto, e assim por diante.

A escolha do vetor de inicialização é bastante importante para não ter muitos blocos de textos cifrados com o mesmo IV.

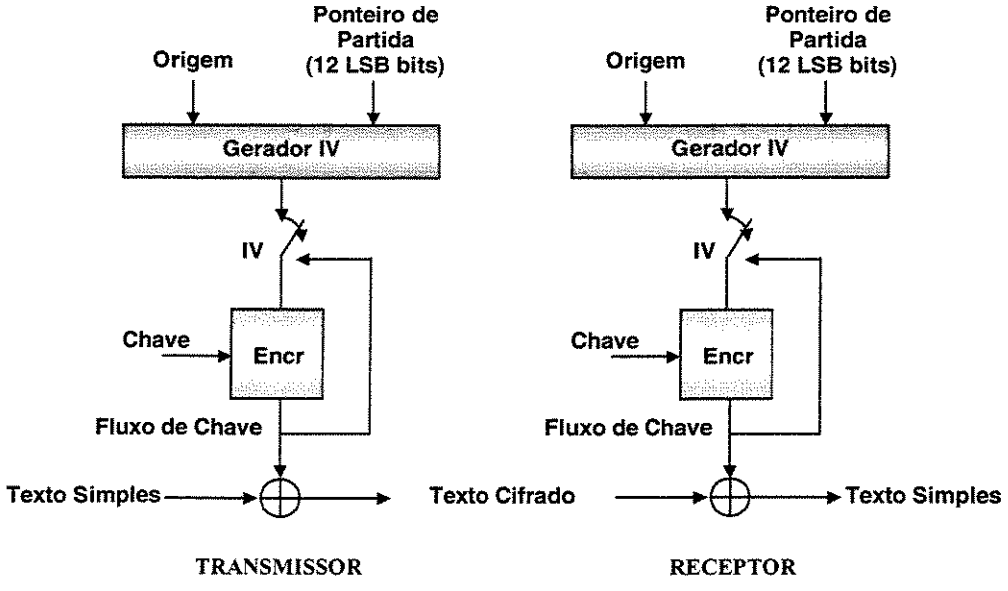


Figura 46 - Encriptação / Decriptação nos sistemas HiperLAN/2

As caixas intituladas "Encr" representam as caixas DES. No primeiro passo, o IV é encriptado; nos passos seguintes, a produção DES é realimentada na caixa de encriptação, como é evidenciado na Figura 45 [JOBMANN+]. O texto cifrado é gerado por operações de XOR.

No receptor, a mesma produção é executada. A encriptação e a decriptação são, aliás, 100% simétricas. Isso está claro na Figura 45, pois a geração do texto cifrado é feita por operações de XOR e, executar uma operação XOR duas vezes é igual à operação inversa. Se os *bits* recebidos são XORed com o mesmo fluxo de *bits* que a encriptação, o resultado é o texto simples.

Em HiperLAN/2, a encriptação do tráfego nas conexões RF é importante para proporcionar proteção contra as escutas às escondidas e ataques do tipo *man-in-the-middle*.

7.2.2 Segurança nos Sistemas HomeRF

O HomeRF é um padrão para redes sem fio desenvolvido por um consórcio de indústrias (Compaq, IBM, Intel, Motorola, etc) chamado HomeRF *Working Group* [MYERS]. É um protocolo totalmente voltado para redes domésticas, podendo operar em redes ad hoc ou em redes estruturadas, com ponto de acesso central.

O objetivo principal do HomeRF *Working Group*, ao projetar o HomeRF, era permitir que os dispositivos de acesso a redes sem fios trabalhassem com voz, dados e canais multimídia através da Internet ou de forma local.

Além de oferecer aspectos técnicos sólidos, simplicidade, segurança e facilidade de uso, a rede HomeRF foi projetada para possuir preços mais acessíveis aos usuários domésticos do que as demais tecnologias de redes sem fio.

A tecnologia HomeRF se baseia na versão original da técnica de modulação FHSS do 802.11, fornece uma cobertura de aproximadamente 50 metros, suficiente para cobrir uma área de uma casa típica e trabalha com taxas de transmissão de 2,4 Ghz.

A especificação HomeRF, como a maioria dos padrões de interface de rede, descreve, fundamentalmente, as duas camadas mais inferiores das sete que compõem o modelo de rede OSI, como mostrado na Figura 46 [MYERS]. A camada inferior, a camada física PHY, determina as características de custo, taxa de transmissão de dados e alcance. A segunda camada, camada de controle de acesso DCL, define os serviços de dados e atributos como a segurança, *roaming* ou mapeamento para camadas superiores padrão.

O HomeRF utiliza o protocolo SWAP (*Shared Wireless Access Protocol*) [NEGUS+], onde as interfaces se comunicam diretamente, sem o uso de um ponto de

acesso. Por um lado, isso diminui o custo da rede, mas por outro, compromete o alcance do sinal.

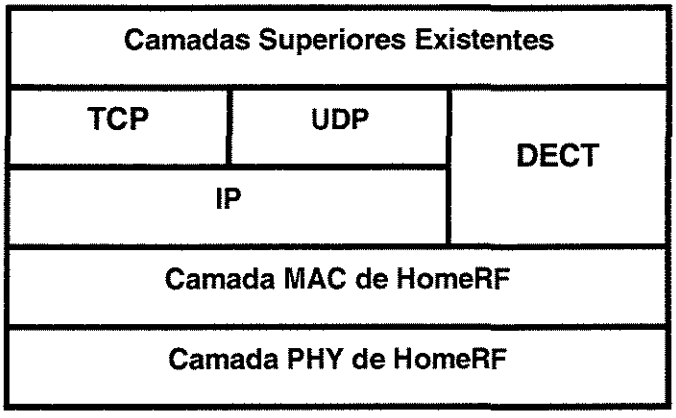


Figura 47 - Camadas de Rede de HomeRF

O modelo de segurança do HomeRF é relativamente transparente e seguro para o usuário final. Ele utiliza a tecnologia de saltos de freqüência, que faz com que o canal de dados se desloque de uma freqüência para outra, dificultando as escutas às escondidas na rede. HomeRF também introduziu o conceito de "senha de rede", necessária para a comunicação dos periféricos com a rede.

Três aspectos de segurança das redes HomeRF serão abordados a seguir e comparados com outros padrões: o comprometimento dos dados, o acesso não autorizado e a negação dos serviços [CHANDRAMOULI2002], [HOMERF].

Comprometimento dos Dados

O padrão HomeRF define uma chave de encriptação de 128 *bits*, usa um vetor de inicialização (IV) de 32 *bits* e determina o tempo de repetição do IV para aproximadamente meio ano. Ele especifica o procedimento de gerência do IV designado para minimizar a possibilidade de repetição do IV.

Acesso não Autorizado

Todos os dispositivos compatíveis com o padrão HomeRF usam um identificador de rede (NWID) "secreto compartilhado" e estes não podem se comunicar sem possuir o NWID. HomeRF também utilizam uma camada física de saltos de freqüência; portanto, um

dispositivo cliente, para sincronizar sua seqüência de saltos com o ponto de acesso, precisa ter o NWID de segurança correto em ordem dos dados recebidos. Sem o NWID, um dispositivo não autorizado nunca conseguirá sincronizar, excluindo a recepção de dados aéreos.

O processo de conexão segue os seguintes passos:

1. O nó escolhe uma freqüência fixa e escuta nela durante um período de tempo;
2. Os pacotes são entregues às camadas mais elevadas do protocolo da subcamada de acesso ao meio (MAC) se:
   - O NWID do receptor corresponder com o NWID do transmissor, e
   - O transmissor for designado a "ensinar" o NWID (requer intervenção manual) e o transmissor, a compreendê-lo.
3. Com exceção da direção de "ensinar/compreender" o NWID, um dispositivo obtém o NWID através da entrada manual feita pelo administrador.
4. O NWID de 24 *bits* impede essencialmente o acesso não autorizado ao fluxo de dados, uma vez que o cliente e o ponto de acesso se associam.

Torna-se praticamente impossível a utilização de dispositivos comercialmente disponíveis para as escutas às escondidas em redes HomeRF, pois aqui, os saltos de freqüência não são estáticos, o que os difere dos sistemas 802.11. De fato, o equipamento próprio para a realização das escutas deveria conseguir encontrar a seqüência de saltos HomeRF e, subseqüentemente, adquirir o sinal e processá-lo, para finalmente decodificar o NWID para uma rede particular.

Negação de Serviço

Através da combinação de saltos de freqüência, uma freqüência diferente para a maioria dos pontos de acessos dentro de uma área ajusta-se em todo momento dado e, pelo fato de que pela camada MAC não transita pacotes de IDs de rede externa, um ataque em larga escala seria virtualmente impossível num ambiente HomeRF.

Devido à existência das vulnerabilidades, é sempre bom fornecer proteção extra ao comprometimento dos dados, através de estratégias de proteção das camadas mais elevadas, como a encriptação direta dos dados ou o uso de VPNs. Se aplicadas corretamente, tais técnicas podem ser eficazes mesmo se a camada física for vulnerável a ataques.

Entretanto, redes como as HomeRF foram projetadas para fornecer razoável garantia de confidencialidade, autenticidade e integridade, sem o uso de contramedidas.

7.3 Outro Padrão para WPAN: IrDA

IrDA (*Infrared Data Association*) e *Bluetooth* são duas tecnologias diferentes para conectividades *wireless* de pequeno alcance que caracterizam as WPAN. Cada uma das tecnologias possui vantagens e desvantagens próprias, mas nenhuma delas aproxima-se da solução ideal para a necessidade de todos os usuários.

Apresentaremos, a seguir, algumas características da tecnologia IrDA.

7.3.1 Segurança nos Sistemas IrDA

O padrão IrDA é uma tecnologia *wireless* definida pelo IrDA *Consortium*, organização não lucrativa composta por membros de mais de 160 companhias que representam computadores pessoais e telefones móveis e especifica meios para transferir dados via radiação infravermelha [VINES2002]. Os aparelhos dos assistentes digitais pessoais (PDAs) ou os notebooks trocam dados através do IrDA com outros aparelhos, como por exemplo, um telefone. PDAs ou notebooks, assim como telefones móveis, suportam um acesso móvel à Internet ou outros serviços de dados. A ligação pode ser estabelecida através do modo normal de dados GSM (com 9.600 ou 14.400 *bits*/s), ou também pelo HSCSD ou GPRS. Para isso, o telefone móvel não pode apenas dispor de uma interface IrDA, mas deve também estar equipado com um "modem GSM". Do ponto de vista do PDA ou do notebook, o telefone móvel comporta-se como se fosse um modem normal.

No geral, IrDA é usado para fornecer conectividade sem fio aos dispositivos que normalmente usam cabos para se conectar. Ele é ponto-a-ponto, com ângulo estreito (30°), o padrão de transmissão de dados ad hoc é designado para operar acima da distância de 0 a 1 metro e alcança velocidades de 9600 bps a 16 Mbps.

As especificações IrDA incluem padrões tanto para os dispositivos físicos quanto para os protocolos utilizados na sua intercomunicação. Dois grandes grupos de protocolos são definidos para suportar a comunicação *wireless* usando a luz infravermelha: IrDA DATA – padrão de dados de IrDA e IrDA CONTROL – padrão de controle de IrDA.

O IrDA DATA consiste num sistema de transmissão de dados ponto-a-ponto orientado a arquivos recomendado para curtas distâncias e altas velocidades de transmissão. Opera com alcance máximo de 1 metro e velocidades de 9600 bps a 16 Mbps.

O IrDA CONTROL consiste numa arquitetura orientada a comando e controle para a comunicação de um *host device* com dispositivos de entrada sem fio, como mouses,

teclados, etc. É um sistema especificamente orientado a *control data packets* e não a arquivos. Seu propósito é passar pequenos pacotes de controle entre um dispositivo *host* e um dispositivo de entrada remoto. Opera com alcance máximo de 7 metros e velocidade de transmissão de até 75 kbps.

Os protocolos dos dados de IrDA são compostos por um conjunto dos protocolos requeridos e por protocolos opcionais. A pilha de protocolos é mostrada na Figura 47 [IrDA].

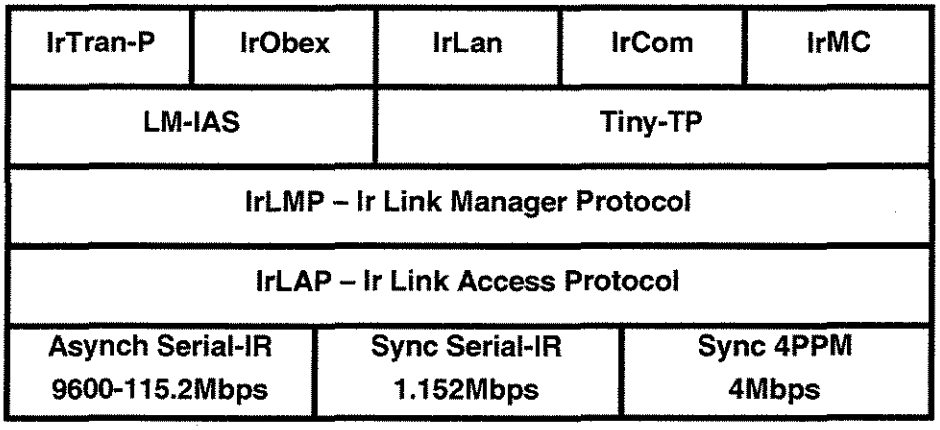


Figura 48 - Pilha de Protocolos do Padrão de Dados de IrDA

Os protocolos mínimos requeridos são [VELASQUEZ2000]:

- PHY (Camada Física) – especifica características óticas, codificação dos dados e o suporte a várias velocidades.
- IrLAP (*Link Access Protocol*) – estabelece uma conexão básica confiável (semelhante ao protocolo IP).
- IrLMP (*Link Manager Protocol*) – faz multiplexamento de serviços e aplicações na conexão fornecida pelo LAP.
- IAS (*Information Access Service*) – provê serviços de informações sobre protocolos e serviços.

Os protocolos opcionais são os seguintes [VELASQUEZ2000]:

- Tiny-TP – fornece o controle de fluxo em conexões de IrLMP com um serviço opcional de segmentação e de remontagem.
- IrCOMM – fornece emulação da porta COM (serial e paralela) para aplicações COM, impressoras e dispositivos modem.

- IrOBEX – fornece os serviços de troca de objetos similares ao HTTP.
- IrDA Lite – fornece métodos de redução do tamanho do código de IrDA ao manter a compatibilidade com implementações completas.
- IrTran-P – fornece o protocolo de troca de imagem usado em dispositivos de captação de imagem digital, como as câmeras.
- IrMC – especificações de como os telefones móveis e dispositivos de comunicação podem trocar informação.
- IrLAN – descreve o protocolo usado para suportar o acesso *wireless* IR às redes de áreas locais.

De acordo com a Figura 48, o modelo básico de uso IrDA é composto por dois dispositivos: o primário (*master*) e o secundário (*slave*) [MEGOWAN+1998]. A tarefa do dispositivo primário é selecionar um dispositivo dentro do seu espaço virtual, estabelecer e manter a conexão virtual. A regra para o dispositivo secundário é somente responder a algum chamado.

Numa típica operação IrDA, o primário inicia o serviço de descoberta do dispositivo e explora o espaço infravermelho (IR) próximo para outros dispositivos. Ele então seleciona um dispositivo dentre os disponíveis e tenta estabelecer a conexão. Durante o estabelecimento da conexão, os dois dispositivos negociam os melhores parâmetros de conexão possíveis baseados nas suas capacidades, na tentativa de se comunicar em velocidades de transmissão comuns mais altas para a otimização e confiabilidade da conexão.

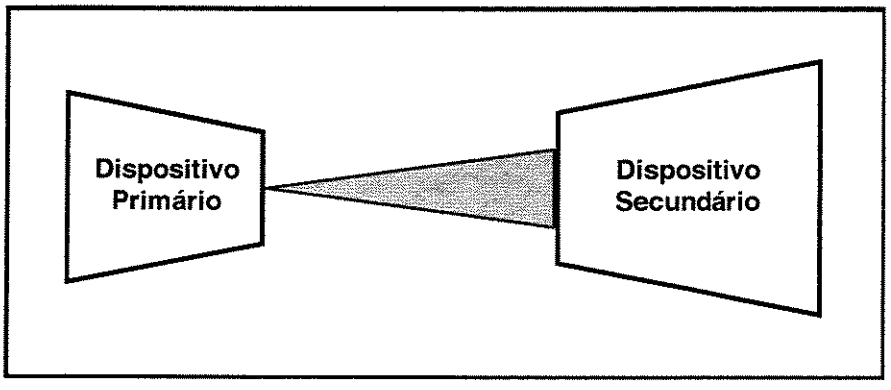


Figura 49 - Modelo Básico de Uso IrDA

Uma vez estabilizada a conexão, aplicações em ambos os lados da conexão podem começar a transferir dados, e também, os dispositivos são capazes de procurar serviços de outros dispositivos.

A natureza direcional de IR impõe uma forma de segurança de baixo nível para a transferência dos dados, porque isso requer o *line-of-sight* ("linha de vista") direto entre o transmissor e o receptor, ou seja, ambos os dispositivos que estiverem se comunicando entre si precisam ter suas portas IR alinhadas. Entretanto, é possível, numa conversação, escutar as escondidas detectando a luz refletida e filtrando para fora o barulho do ambiente adjacente. IrDA não fornece potencialidades de segurança no nível de ligação, como ocorre em *Bluetooth*. Em vez disso, IrDA confia na camada superior de protocolos e aplicações para proporcionar autenticação e/ou encriptação.

Os espaços de aplicação de *Bluetooth* e IrDA se sobrepõem: muitas das aplicações definidas para IrDA também são definidas para *Bluetooth* e, em algumas situações, o uso de IrDA é melhor para a transmissão de dados do que *Bluetooth*, e vice-versa. A troca de dados é considerada uma função fundamental tanto para o *Bluetooth* quanto para o IrDA.

7.4 Análise Comparativa entre outros Padrões de WWAN, WLAN e WPAN nos Aspectos de Segurança

Como tecnologias que caracterizam as WWAN, foram abordados três sistemas de telefonia celular: GSM, GPRS e UMTS. Analisando os aspectos básicos de segurança, especialmente os requisitos de confidencialidade, autenticação e disponibilidade, conclui-se que elas possuem poderosos mecanismos de segurança inerentes à própria camada física, como as técnicas de autenticação e privacidade que utilizam algoritmos de criptografia , o que garante ainda mais a segurança destes sistemas.

Apesar da garantia de segurança, as redes GSM, GPRS e UMTS estão expostas aos riscos de segurança. Geralmente, os ataques visam explorar vulnerabilidades nos algoritmos e protocolos de segurança e, os que se tornaram mais evidentes, concentram-se principalmente nas redes GSM. Em GPRS, como os seus algoritmos são mantidos em sigilo, os ataques ainda não são conhecidos e disponibilizados. Em UMTS, as principais vulnerabilidades ocorrem devido aos ataques encontrados nas redes fixas.

Na Tabela 1, apresentamos um resumo dos aspectos de segurança dos principais sistemas móveis, GSM, GPRS e UMTS.

	GSM	GPRS	UMTS
Mecanismos de autenticação	Procedimento de desafio/resposta baseado em uma chave secreta de autenticação compartilhada por duas entidades.	Procedimento de desafio/resposta baseado em uma chave secreta de autenticação compartilhada por duas entidades.	Procedimento de desafio/resposta baseado na autenticação mútua entre o usuário e a rede, que passa a conhecer a chave secreta compartilhada entre eles.
Mecanismos de confidencialidade da identificação	Usa criptografia e procedimentos de identificação temporal.	Usa criptografia e procedimentos de identificação temporal.	Usa criptografia e procedimentos de identificação temporal.
Mecanismos de confidencialidade dos dados	Utiliza o algoritmo de *stream cipher* A5, que encripta cada caractere de uma seqüência.	Utiliza o algoritmo GEA (ou GPRS/A5), que realiza todo o ciframento na camada superior, sendo mais adequado à comutação de pacotes.	Utiliza o algoritmo de *stream cipher* f8. Ao contrário dos algoritmos A5 e GEA, que têm tamanho de chave de 54 *bits*, o f8 têm chave de 128 *bits*.
Garantia de integridade	Não	Não	Utiliza o algoritmo f9, padronizado para todo o sistema UMTS.
Estabelecimento das chaves	Utiliza o algoritmo A8. Ele é executado dentro do SIM-Card e da AUC, as duas únicas entidades que conhecem a chave secreta Ki	Utiliza o algoritmo A8. Ele é executado dentro do SIM-Card e da AUC, as duas únicas entidades que conhecem a chave secreta Ki	Utiliza o algoritmo f3 para gerar a chave de cifragem que garante confidencialidade, e f4 para gerar a chave para o algoritmo de integridade. As redes UMTS garantem que as chaves geradas não foram recentemente usadas.

Tabela 1 - Comparação dos aspectos de segurança das redes GSM, GPRS e UMTS

As tecnologias IEEE 802.11, HiperLAN e HomeRF especificam um conjunto de padrões que os definem como tecnologias de LAN sem fio (WLAN).

Embora as vantagens desses sistemas sejam inúmeros, a segurança é uma das grandes preocupações em WLAN, principalmente em aplicações *m-commerce* e *e-commerce*, e a mobilidade, apesar de benéfica, aumenta os riscos de segurança nessas redes. As soluções de segurança implementadas nas tecnologias comercialmente disponíveis ainda não são suficientemente robustas para garantir a integridade da rede.

As redes WLAN utilizam técnicas de autenticação e encriptação dos dados como forma de proporcionar segurança a seus usuários. Alguns problemas de segurança relacionados a confidencialidade, integridade e disponibilidade mostram que as tecnologias

em questão possuem falhas, o que possibilita cada vez mais a ação dos *hackers*.

Na Tabela 2, será mostrada a implementação da segurança nas redes 802.11, HiperLAN/2 e HomeRF.

	802.11	HiperLAN/2	HomeRF
Autenticação	É baseada em dois métodos: um criptográfico e outro não. O método não-criptográfico possui duas maneiras (métodos aberto e fechado) de identificação de um cliente sem fio. Ambos os métodos são considerados primitivos e extremamente vulneráveis. O método criptográfico utiliza chaves compartilhadas para autenticar o cliente no AP. Esse método não consegue autenticar o AP para o cliente.	Utiliza esquemas opcionais de chaves pré-compartilhadas ou chaves públicas.	Utiliza um mecanismo baseado em um identificador de rede (NWID) secreto. Esse mecanismo é aliado ao mecanismo de saltos de freqüência de HomeRF.
Confidencialidade dos dados	Utiliza o método criptográfico WEP, baseado no algoritmo RC4. Os tamanhos do vetor de inicialização e da chave secreta compartilhada utilizada são, respectivamente, de 24 *bits* e 40 *bits*.	Utiliza chaves de encriptação de 56 *bits* e 168 *bits* baseadas no algoritmo criptográfico DES.	Utiliza a combinação de uma chave de encriptação de 128 *bits* com um vetor de inicialização (IV) de 32 *bits* para gerar a criptografia final. Funciona como um "randomizador" de chaves, repetindo-se em cerca de meio ano.

Tabela 2 - Comparação dos aspectos de segurança das redes 802.11, HiperLAN/2 e HomeRF

As tecnologias *Bluetooth* e IrDA caracterizam as redes WPAN. O *Bluetooth* apresenta vantagens sobre IrDA nos aspectos de mobilidade e segurança. Globalmente, *Bluetooth* é mais versátil que o IrDA, pois outros protocolos como o WAP podem ser adicionados à pilha de protocolos *Bluetooth* para aumentar suas funcionalidades.

Segundo [SUVAK1998] e [SUVAK2000], é possível comparar as tecnologias IrDA e *Bluetooth* em alguns aspectos, como o meio sem fio utilizado, mobilidade, segurança e taxa de transmissão dos dados, com o objetivo de entender suas diferenças e saber em que aspectos elas se sobrepõem.

A competição entre as duas tecnologias continuará existindo desde que nenhuma delas já tenha satisfeito as necessidades de todos os usuários.

A Tabela 3 resume os critérios de comparação das tecnologias:

	IrDA	*Bluetooth*
Meio sem fio utilizado	Utiliza comunicação direta infravermelha. Ela é direcional e requer *line-of-sight* direto entre os dispositivos, ou seja, exige que o usuário esteja ativamente engajado na transferência da informação. O principal problema das comunicações IR é o bloqueio do sinal por objetos opacos.	Utiliza comunicação de rádio freqüência. Ela é omni-direcional e a transmissão acontece através de sólidos, objetos não-metais. Conseqüentemente, os usuários não precisam estar ativamente envolvidos na comunicação dos dispositivos. O maior inconveniente nas comunicações RF é a possibilidade de escutas maliciosas nos dispositivos *Bluetooth*.
Mobilidade	Fornece pouca mobilidade. Para manter a comunicação, o transmissor infravermelho precisa estar a uma distância máxima de um metro, numa localização fixa e posicionado em direção aproximada do outro dispositivo.	Mobilidade máxima. Numa rede *Bluetooth*, o usuário pode se movimentar por perto com o dispositivo que a comunicação procede sem interrupção, proporcionando, ao usuário, permanecer dentro do alcance.
Segurança	Provê uma forma de segurança de baixo nível. Requer um *line-of-sight* direto entre o transmissor e o receptor, ou seja, o direcionamento do dispositivo com o receptor desejado garante a segurança na transmissão dos dados. IrDA não fornece segurança no nível da ligação; ele confia em protocolos de camadas superiores e aplicações para proporcionar autenticação e/ou encriptação.	Proporciona autenticação e encriptação como formas de segurança. A autenticação é baseada no protocolo de desafio-resposta usando uma chave secreta (*password* ou PIN). Ambos os dispositivos contém a mesma chave secreta. Para adicionar segurança, a transmissão só pode ser encriptada depois que os dispositivos são autenticados.
Taxa de transmissão dos dados	IrDA suporta taxas de transmissão de dados superior a 4 Mbps.	A banda larga agregada aos dispositivos *Bluetooth* é limitada a 1 Mbps.

Tabela 3 - Resumo dos Critérios de Comparação das Tecnologias IrDA e *Bluetooth*

Os padrões apresentados neste trabalho englobam as mais comuns e promissoras tecnologias sem fios existentes. Esses padrões competem um com outro em algumas áreas, enquanto se complementam em outras. Além do mais, muitos desses padrões e tecnologias se sobrepõem, significando que poderemos ver a sobrevivência de mais das tecnologias competitivas.

Capítulo 8

Conclusão

A tecnologia *wireless* criou uma dimensão completamente nova nas práticas de computação e de negócios que possibilitaram as empresas oferecer uma série de funcionalidades para a troca de informações, tais como a facilidade de mobilidade de dispositivos e flexibilidade de conexões.

A mobilidade permite que usuários com acessos às redes públicas e privadas possam permanecer conectados em qualquer lugar dentro da área de cobertura. A flexibilidade diz respeito à facilidade de conexão dos dispositivos sem a necessidade de uma estrutura física de fios.

Atualmente, para o acesso às redes *wireless*, são utilizados três categorias diferentes de tecnologias de comunicação sem fios, sendo:

- redes WWAN (*Wireless Wide Area Network*) definidas pelas tecnologias GSM, GPRS e UMTS;
- redes WLAN (*Wireless Local Area Network*) definidas pelos padrões IEEE 802.11, HiperLAN/2 e HomeRF;
- redes WPAN (*Wireless Personal Area Network*) definidas pelos padrões *Bluetooth* e IrDA.

A crescente utilização e popularização das redes sem fios trouxe, além de inúmeros benefícios e vantagens para seus usuários, uma maior preocupação com a segurança. Nessas redes, a segurança das informações é fundamental, pois todos os usuários podem acessar os recursos livremente sem ter o limite dos cabos. O controle de acesso e a confidencialidade devem ser sempre garantidos.

Algumas características de segurança física, como o controle do sinal transmitido, utilização de dispositivos de controle do meio e controle de acesso físico, presentes nas redes cabeadas inexistem nas redes sem fios, o que as tornam menos seguras às invasões e aos ataques.

Para proporcionar maior proteção às redes *wireless*, é necessário adicionar mecanismo de autenticação de dispositivos e confidencialidade dos dados. É a camada de enlace de dados das redes sem fios que deve prover características de segurança que compatibilizem as conexões com e sem fios, e possibilitem a execução de aplicativos sem

riscos.

Sob o aspecto técnico, as redes sem fios apresentam uma série de vulnerabilidades oriundas da própria concepção das tecnologias. A melhor forma de adicionar segurança a esses ambientes é através do planejamento e execução de uma estratégia inteligente de segurança específica para as redes *wireless*, antecipando as exigências de segurança futuras e integrando tais considerações em cada etapa do processo de desenvolvimento.

A estratégia específica para as redes sem fios deve definir a configuração cuidadosa dos equipamentos utilizados; quais equipamentos são permitidos; que tipos de dados podem ser transferidos na rede e se é obrigatório o uso de métodos de criptografia e autenticação, etc; o uso de equipamentos específicos para proporcionar a confidencialidade dos dados das camadas superiores, como roteadores VPN; manter registros das atividades na rede e sistemas de detecção de intrusão, entre outros.

Apesar de todas as medidas de segurança existentes e já citadas, nenhum ambiente *wireless*, atualmente, é totalmente seguro, pois ataques bem sucedidos são possíveis e conhecidos. O surgimento de novas vulnerabilidades e os mecanismos existentes nos dias de hoje são contornáveis com relativa facilidade por um atacante motivado.

Por este motivo, os estudos e pesquisas na área de segurança em redes sem fios devem continuar, com o propósito de oferecer melhorias nas tecnologias existentes e torná-las mas rápidas, menores, mas baratas e mais seguras. A expectativa é que aconteça uma padronização crescente no mundo *wireless*, no sentido de tornar as arquiteturas de soluções de segurança menos tediosas e favorecer sua divulgação e aceitação.

Com a evolução veloz das tecnologias, o mercado *wireless* sempre será redefinido, fazendo com que as pesquisas na área de segurança também tomem rumos diferentes. Os mesmos princípios de segurança serão aplicados, mas é certa a continuidade de novos e emocionantes obstáculos a escalar.

Neste trabalho apresentamos características de diferentes tecnologias de redes sem fios encontradas na literatura, o que nos permitiu obter uma visão geral dos sistemas *wireless* existentes.

Como contribuição deste trabalho ressaltamos um estudo detalhado e comparativo dos aspectos de segurança das tecnologias de redes sem fios, algo que se mostrou difícil de se encontrar no início dos nossos trabalhos.

Glossário de Siglas

ACO	-	Authenticated Cipher Offset
ADSL	-	Asymmetric Digital Subscriber Line
AH	-	Authentication Header
AM	-	Amplitude Modulation
AMPS	-	Advanced Mobile Phone System
AP	-	Access Point
ARFCN	-	Absolute Radio Frequency Channel Number
ATM	-	Asynchronous Transfer Mode
AuC	-	Authentication Center
BD_ADDR	-	Bluetooth Device Address
BS	-	Base Station
BSA	-	Basic Service Area
BSC	-	Base Station Controller
BSS	-	Basic Service Set
BTS	-	Base Transceiver Station
BWA	-	Broadband Wireless Access
CDMA	-	Code Division Multiple Access
CDPD	-	Cellular Digital Packet Data
CK	-	Cipher Key
CRC	-	Cyclic Redundancy Check
DES	-	Data Encryption Standard
DS	-	Distribution System
DSSS	-	Direct Sequence Spread Spectrum
EAP	-	Extensible Authentication Protocol
EDGE	-	Enhanced Data rates for Global Evolution
EIR	-	Equipment Switching Center
ERB	-	Radio Base Station
ESCE	-	External Security Control Entity
ESP	-	Encapsulating Security Protocol

ESS - Extended Service Set

ETSI - European Telecommunications Standards Institute

FDD - Frequency Division Duplex

FDM - Frequency Division Multiplexing

FDMA - Frequency Division Multiple Access

FEC - Forward Error Correction

FHSS - Frequency Hopping Spread Spectrum

FM - Frequency Modulation

GEA-GPRS - GPRS Encryption Algorithm

GGSN - Gateway GPRS Support Node

GMSK - Gaussian Minimum Shift Keying

GPRS - General Packet Radio Service

GSM - Global System for Mobile Communications

HiperLAN - High Performance Radio LAN

HLR - Home Location Register

HomeRF - Home Radio Frequency

HSCSD - High Speed Circuit Switched Data

HTTP - Hyper Text Transfer Protocol

I-ADD - Identify targets and roles, Analyze attacks and vulnerabilities, Define strategies and Design secutity

IAS - Information Access Service

ICN-IWU - Intercore Network Interworking Units

ICV - Integrity Check Value

IDC - International Data Corporation

IEEE - Institute of Electrical and Eletronic Engineers

IKE - Internet Key Exchange

IMEI - International Mobile Equipment Identify Code

IMSI - International Mobile Subscriber Identify

IP - Internet Protocol

IPSec - Secure Internet Protocol

IPX - Internet Packet Exchange

IR	-	Infrared
IrDA	-	Infrared Data Association
IrLAP	-	Infrared Link Access Protocol
IrLMP	-	Infrared Manager Protocol
ISP	-	Internet Service Provider
IV	-	Initialization Vector
IWU	-	Interworking Units
KG	-	Key Generator
L2CAP	-	Logical Link Control and Adaptation Protocol
LAI	-	Location Area Identify
LFSR	-	Linear Feedback Shift Register
LMDS	-	Local Multipoint Distribution System
LR	-	Location Register
MAN	-	Metropolitan Area Network
MS	-	Mobile Station
MSC	-	Mobile services Switching Center
MT	-	Mobile Terminal
NIC	-	Network Interface Card
NSS	-	Network Subsystem
NWID	-	Network ID
OFB	-	Output Feedback
OFDM	-	Orthogonal Frequency Division Modulation
P2P	-	Peer to Peer
PCMCIA	-	Personal Computer Memory Card International Association
PCN	-	Personal Communications Network
PDA	-	Personal Digital Assistant
PHY	-	Physical Layer
PIN	-	Personal Identification Number
PRNG	-	Pseudo-random Number Generator
QoS	-	Quality of Service
RAI	-	Routing Area Identify

RC4	-	Rivest Code 4
RF	-	Radio Frequency
RNG	-	Random Number Generator
SAFER	-	Secure And Fast Encryption Routine
SDA	-	Smartcard Developer Association
SGSN	-	Serving GPRS Support Node
SIG	-	Special Interest Group
SIM	-	Subscriber Identify Module
SMS	-	Short Message Service
SN	-	Service Network
SRES	-	Signed Response
SSID	-	Service Set Identifier
STA	-	Stations
SWAP	-	Shared Wireless Access Protocol
TA	-	Terminal Adapter
TCP/IP	-	Transmission Control Protocol / Internet Protocol
TDD	-	Time Division Duplex
TDM	-	Time Division Multiplexing
TDMA	-	Time Division Multiple Access
TE	-	Terminal Equipment
TKIP	-	Temporal Key Integrity Protocol
TLLI	-	Temporary Logical Link Identify
TMSI	-	Temporary Mobile Subscriber Identify
UEA	-	UMTS Encryption Algorithm
UMTS	-	Universal Mobile Telecom System
URAN	-	UMTS Radio Access Network
USB	-	Universal Serial Bus
USIM	-	User Subscriber Identify Module
VLR	-	Visitor Location Register
VPN	-	Virtual Private Network
WAP	-	Wireless Application Protocol

WCDMA	-	Wideband CDMA
WEP	-	Wired Equivalent Privacy
WEP2	-	Wired Equivalent Privacy 2
Wi-Fi	-	Wireless Fidelity
WLAN	-	Wireless Local Area Network
WLL	-	Wireless Local Loop
WMAN	-	Wireless Metropolitan Area Network
WPA	-	Wi-Fi Protected Access
WPAN	-	Wireless Personal Area Network
WWAN	-	Wireless Wide Area Network

Referências Bibliográficas

[AGRAWAL+1999] AGRAWAL, P., SREENAN, C. J., Get *Wireless: A Mobile Technology Spectrum*. IEEE IT Professional Magazine, vol. 1, no. 4, pp. 18-23, 1999.

[ANAND2001] ANAND, Nikhil. *An Overview of Bluetooth Security*. SANS Institute, 2001. http://giac.org/practical/gsec/Nikhil_Anand_GSEC.pdf (referenciado Março 2003)

[ANTIPOLIS2002] ANTIPOLIS, Sophia. *GSM calls even more secure thanks to new A5/3 Algorithm*. July 01/2002. http://www.gsmworld.com/news/press_2002/press_15.shtml (referenciado Março 2003)

[BORISOV+2001] BORISOV, N., GOLDBERG, I., WAGNER, D., *Intercepting Mobile Communications: The Insecurity of 802.11*. 7th Annual International Conference on Mobile Computing and Networking, 2001. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf (referenciado Março 2003)

[BREWER+] BREWER, E., BORISOV, N., GOLDBERG, I., WAGNER, D. *Security of WEP Algorithm*. Internet Security, Applications, Authentication and Cryptography (ISAAC). Computer Science Division. University of California, Berkeley. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (referenciado Março 2003)

[BRICENO+01] BRICENO, M., GOLDBERG, I., WAGNER, D. *An Implementation of COMP128*. http://www.iol.ie/~kooltek/a3a8.txt (referenciado Março 2003)

[BRICENO+02] BRICENO, M., GOLDBERG, I., WAGNER, D. *GSM Cloning*. http://www.isaac.cs.berkeley.edu/isaac/gsm.html (referenciado Março 2003)

[BRICENO+03] BRICENO, M., GOLDBERG, I., WAGNER, D. *A pedagogical Implementation of A5/1*. http://packetstormsecurity.nl/crypt/cryptanalysis/a51-pi.htm (referenciado Março 2003)

[BRICENO+04] BRICENO, M., GOLDBERG, I., WAGNER, D. *A Pedagogical Implementation of A5/1 e A5/2.* http://cryptome.org/gsm-a512.htm (Referenciado Março 2003)

[BROOKSON2001] BROOKSON, Charles. *GPRS Security*. Dec., 2001. http://www.brookson.com/gsm/gprs.pdf (referenciado Agosto 2003)

[CDMA] CDMA Development Group web site. http://www.cdg.org (referenciado Janeiro 2003)

[CHANDRAMOULI2002] CHANDRAMOULI, Vijay. *A Detailed Study on Wireless Lan Technologies*. Department of Computer Science and Engineering, The University of Texas at Arlington. http://crystal.uta.edu/~kumar/cse6392/termpapers/Vijay_paper.pdf (referenciado Agosto 2003)

[DORNAN2002] DORNAN, Andy, *The Essential Guide to Wireless Communications Applications*. New Jersey: Editora Prentice Hall PTR, 2002.

[EKLUND+2002] EKLUND, C., MARKS, R. B., STANWOOD, K. L. & WANG, S. *IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access*. IEEE Communications Magazine, pp. 98-107, June 2002. http://www.ieee.802.org/16/docs/02/C80216-02_05.pdf (referenciado Dezembro 2003)

[FLUHRER+2001] FLUHRER, S., MANTIN, I., SHAMIR, A. *Weakness in the Key Scheduling Algorithm of RC4*. Cisco Systems, Inc. Computer Science Department, The Weizmann Institute, Israel, 2001. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (referenciado Março 2003)

[FORMAN+1994] FORMAN, G., ZAHORJAN, J. *The Challenges of Mobile Computing*. IEEE Computer Journal, vol. 27, no. 4, pp. 38-47, April 1994

[HOMERF] HomeRF Working Group, Inc. *A Comparision of Security in HomeRF versus IEEE 802.11b.* http://www.palowireless.com/homerf/docs/security_comparision.pdf (referenciado Agosto 2003)

[IEEE] Institute of Electrical and Electronics Engineers. *The IEEE 802.16 Working Group on Broadband Wireless Access Standards*.

http://www.ieee802.org/16/ (referenciado Outubro 2003)

[IrDA] The Infrared Data Association web site. *Technical Summary of "IrDA DATA" and "IrDA CONTROL".* http://www.irda.org/standards/standards.asp (referenciado Agosto 2003)

[ITU] *Intenational Telecommunications Union* web site. http://www.itu.int/ (referenciado Janeiro 2003)

[JOBMANN+] JOBMANN, K., RADIMIRSCH, M. *HiperLAN/2*. Institut für Allgemeine Nachrichtentechnik, University of Hannover. http://www.kbs.uni-hannover.de/~allert/hiperLAN/ (referenciado Agosto 2003)

[JOHNSSON1999] JOHNSSON, Martin. *HiperLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band*. HiperLAN/2 Global Forum, 1999. http://www.hiperLAN2.com/presdocs/site/whitepaper.pdf (referenciado Agosto 2003)

[KARAOGUZ2001] KARAOGUZ, Jeyham, *High-Rate Wireless Personal Area Networks*. IEEE Communications Magazine, vol. 39, no. 12, December 2001, pp. 96-102.

[KARYGIANNIS+2002] KARYGIANNIS, T., QWENS L., *Wireless Network Security – 802.11, Bluetooth and Handheld Devices*. NIST (National Institute of Standards and Technology) Special Publication 800-48, 2002. http://csrc.nist.gov/publications/drafts.html (referenciado Março 2003)

[LANGNES2001] LANGNES, Runar, *UMTS Security Architecture*. Telenor R&D, 2001. Disponível em http://www.telenor.no/fou/publisering/Not01/sec_UMTS.PDF

[LAUDON+1999] LAUDON, Kanneth C., LAUDON, Jane P., *Gerenciamento de Sistemas de Informação*. Rio de Janeiro: Editora LTC, 1999.

[LORD2003] LORD, Steve. *Modern GSM Insecurities*. The Encyclopedia of Computer Security. An ISS Technical White Paper, 2003. http://www.itsecurity.com/papers/iss8.htm (referenciado Março 2003)

[MARGRAVE] MARGRAVE, David, *GSM Security and Encryption*. http://spyhard.narod.ru/phreak/gsm-secur.html (referenciado Março 2003)

[MATEUS+1998] MATEUS, G. R., LOUREIRO, A. A., *Introdução à Computação Móvel.* 11ª Escola de Computação. COPPE/Sistemas, NCE/UFRJ, 1998.

[MCFARLAND+2003] MCFARLAND, B., WONG M., *The Family Dynamics of 802.11.* ACM Queue, Vol. 1, pp. 28 – 38, May 2003.

[MEGOWAN+1998] MEGOWAN, P. J., SUVAK, D. W., KNUTSON, C. D., *IrDA Infrared Communications: An Overview.* Tech. Report, Counterpoint Systems Foundry, Inc., 1998. http://www.irda.org/use/pubs/Overview.pdf (referenciado Agosto 2003)

[MILLER1999] MILLER, Thomas, *Bluetooth Security Architecture – version 1.0.* Bluetooth White Paper, 1999. http://www.Bluetooth.org/foundry/sitecontent/document/Security_Architecture.pdf (referenciado Março 2003)

[MYERS] MYERS, Eamon. *HomeRF Overview and Market Position.* HomeRF Resource Center. http://www.palowireless.com/homerf/homerf.asp (referenciado Agosto 2003)

[NEGUS+] NEGUS, Kevin J., STEPHENS, Adrian P., LANSFORD, Jim. *HomeRF™: Wireless Networking for the Connected Home.* http://www.cos.ufrj.br/~ferver/cos871/homerf.pdf (referenciado Agosto 2003)

[PEREZ+2003] PEREZ, P., BOLDRINI, R., DAHAB, R. *Aspectos de Segurança das Redes GSM, GPRS e UMTS.* Universidade Estadual de Campinas, Instituto de Computação, 2003.

[RAPPAPORT2001] RAPPAPORT, Theodore S., *Wireless Communications: Principles and Practice.* New Jersey: Editora Prentice Hall PTR, 2001.

[SAIRAM+2002] SAIRAM, K. V. S. S. S. S., GUNASEKARAN, N., REDDY S. Rama, *Bluetooth in Wireless Communication.* IEEE Communications Magazine, vol. 40, no. 6, pp. 90 – 96, 2002.

[SCOURIAS] SCOURIAS, John. *A Brief Overview of GSM.* http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html (referenciado Março 2003)

[SHAMIR+] SHAMIR, A., BIRYUKOV, A., WAGNER, D. *Real Time Cryptanalysis on A5/1*. http://cryptome.org/a5.ps (referenciado Março 2003)

[SOARES+1998] SOARES, L. F. G., LEMOS G., COLCHER, S., *Redes de Computadores: das LANs, MANs e WANs às redes ATM*. Rio de Janeiro: Editora Campus, 1998.

[STALLINGS1999] STALLINGS, William, *Cryptography and Network Security: Principles and Practice*. New Jersey: Editora Prentice Hall PTR, 1999.

[STALLINGS2000] STALLINGS, William, *Network Security Essentials*. New Jersey: Editora Prentice Hall PTR, 2000.

[STALLINGS2002] STALLINGS, William, *Wireless Communication and Networks*. New Jersey: Editora Prentice Hall PTR, 2002.

[STUBBLEFIELD+2001] STUBBLEFIELD, A., IOANNIDIS, J., RUBIN, A. D. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. AT&T Labs Technical Report TD-4ZCPZZ, AT&T Labs 2001. http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf (referenciado Março 2003)

[SUVAK1998] SUVAK, D. W., *IrDA versus Bluetooth: A Complementary Comparision.* Tech. Report, Extended Systems, Inc., 1998. http://www.irda.org/design/ESIIrDA_*Bluetooth*paper.doc (referenciado Agosto 2003)

[SUVAK2000] SUVAK, D. W., *Comparing the benefits of IrDA and Bluetooth. Wireless* System Design, pp. 31-33, 2000. http://www.wsdmag.com/Globals/PlanetEE/Content/592.pdf (referenciado Agosto 2003)

[SWAMINATHA+2002] SWAMINATHA, Tara M., ELDEN, Charles R., *Wireless Security and Privacy: best practices and design techniques.* Boston: Editora Addison-Wesley, 2002.

[TAURION2002] TAURION, Cezar, *Internet Móvel. Tecnologias, Aplicações e Modelos*. Rio de Janeiro: Editora Campus, 2002.

[TRÄSKBÄCK2001] TRÄSKBÄCK, Marjaana. *Security of Bluetooth: An Overview of Bluetooth Security*. Department of Electrical and Communications Engineering, 2001. http://www.cs.hut.fi/Opinnot/Tik-86.174/*Bluetooth*_Security.pdf (referenciado Março 2003)

[UMTS1997] UMTS Forum: *A regulatory framework for UMTS*, 1997. http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/Resources_Reports_01_index (referenciado Agosto 2003)

[VAINIO2000] VAINIO, Juha T. *Bluetooth Security*. Department of Computer Science and Engineering. Helsinki University of Technology, 2000. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html (referenciado Março 2003)

[VINES2002] VINES, Russell Dean. *Wireless Security Essentials – Defending Mobile Systems from Data Privacy*. Indianapolis: Wiley Publishing, Inc., 2002.

[VELASQUEZ2000] VELASQUEZ, Jay. *Wireless Personal Area Networks: A Comparative Look at IrDA-Data and Bluetooth*. April, 2000. http://fiddle.visc.vt.edu/courses/ecpe6504-wireless/projects_spring2000/report_velasquez.pdf (referenciado Agosto 2003)

[WALKER2000] WALKER, Jesse R. *Unsafe at any key size; An Analysis of the WEP encapsulation*. IEEE Document 802.11-00/362, 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (referenciado Março 2003)

[WATKINS2000] WATKINS, David. A., *Overview and Comparison of GSM, GPRS and UMTS*. Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, 2000.