Wilson Vicente Ruggiero

Modelo de segurança para redes Ad-Hoc

Tese apresentada à Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a obtenção do título de Livre Docência no Departamento de Engenharia de Computação e Sistemas Digitais.

Defendida em 5/6/02

nomeado em 1°/8/02

Fevereiro/2002

Índice

GLOSSÁRIO

ABR	Associatively Based Routing
ACL	Asynchronous Connection Less Link
ACO	Authenticated Ciphering Offset
ALP	Adaptive Link State Protocol
AM	Amplitude Modulation
AODV	Ad hoc On Demand Distance Vector
AP	Access Point
BD_ADDR	Bluetooth Address
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
BT	Bluetooth
CA	Certification Authority
COF	Ciphering Offset
CRC	Check Redundancy Cyclic
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DS	Direct Sequence
DSDV	Destination Sequence Distance Vector
DSR	Dynamic Source Routing
ESS	Extended Service Set
FFH	Fast FH
FH	Frequency Hopping
FHSS	Frequency Hop Spread Spectrum
FM	Frequency modulated
FMFB	FM demodulator with feedback
FSR	Fisheys State Routing
GSR	Global State Routing
IBSS	Independent Basic Service Set
IC	Integrated Circuit
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial Scientific Medical
K	Key
LAN	Local Area Network
LANMAR	Landmark Ad hoc Routing
LFST	Linear Feedback Shift Register
LLC	Logical Link Control
LMR	Lightweight Mobile Routing

LRR	Least Resistance Routing
MAC	Medium Access Control
MANET	Mobile Ad hoc NETwork
MDSR	Multipath Dynamic Source Routing
MH	Mobile Hosts
MSDU	MAC Service Data Unit
MSS	Mobile Support Station
NIC	Network Interface Card
OLSR	Optimized Link State Routing
OSI	Open Standard International
PAN	Personal Area Network
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PHY	Physical Layer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLL	Phase Lock Loop
PRNG	Pseudo Random Number Generator
QPSK	Quadrature Phase Shift Keying
RABR	Route Lifetime Assessment Based Routing
RAND	Random
RDMAR	Relative Distance Micro discovery Ad hoc Routing
RF	Radio Frequency
RIP	Routing Internet Protocol
ROAM	Routing On demand Acyclic Multipath
SCO	Synchronous Connection Oriented Link
SFH	Slow FH
SIG	Special Interest Group
SRES	Signed RESponse
SS	Spread Spectrum
SSA	Signal Stability Based Adaptive
SSL	Secure Socket Layer
STA	Station
STAR	Source Tree Adaptive Routing
TCP	Transport Control Protocol
TDD	Time Division Duplex
TH	Time Hopping
TORA	Temporarily Ordered Routing Algorithm
VLAN	Virtual Local Area Network

WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WIM	Wireless Identity Module
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WRP	Wireless Routing Protocol

Resumo

A evolução das redes de computadores e da Internet em especial tem sido muito rápida e produzido enormes avanços não só nos aspectos tecnológicos como econômicos e porque não sociais.
As características dos serviços world wide web da Internet associadas a ubiqüidade da teia mundial produziu um enorme impulso na prestação de serviços on-line e na disponibilização de informações para a sociedade em geral.
Este cenário, onde novos paradigmas surgem para reformular antigos conceitos e permitir que a sociedade possa usufruir adequadamente dos avanços tecnológico, tem provocado profundas mudanças na forma como as pessoas e as entidades interagem entre si.
O advento das comunicações sem fio intensificou ainda mais este efeito. Dentro do ambiente da teia mundial, com a capacidade de comunicação sem fio e a conseqüente mobilidade resultante, pode-se imaginar a amplificação do conceito de "a qualquer instante e em qualquer lugar". Os usuários nessas redes, terão uma característica mais dinâmica, podendo surgir ou desaparecer da rede por simplesmente saírem ou entrarem no raio de alcance das comunicações sem fio. Num ambiente onde se realizam transações comerciais envolvendo um número muito grande de participantes que possam se conectar à rede através de um canal de acesso sem fio ou de uma rede Ad-Hoc, as caraterísticas de mobilidade, ubiqüidade e dinamismo determinam uma comunidade incerta e desconhecida de possíveis participantes ou observadores dos fatos e ações pertinentes as transações sendo realizadas. O dinamismo que permite aos usuários estarem presentes ou ausentes, ou que visitantes desejados e conhecidos ou estranhos e indesejados, possam estar em condições de observar ou mesmo tentar participar das transações sendo realizadas, torna este ambiente extremamente desafiador para a garantia da segurança da informação.
Dentro deste cenário é que se posiciona este trabalho cujo objetivo é a definição de um modelo de segurança para redes Ad-Hoc que contemple variações temporais naturais nas relações de confiança entre seus participantes. Associado a este modelo define-se uma arquitetura de segurança que identifica todos as entidades, relacionamentos, mecanismos, protocolos e serviços necessários para se constituir um ambiente seguro para redes Ad-Hoc.
A característica diferenciadora do modelo de segurança proposta neste trabalho é a forma como os aspectos dinâmicos associados à mobilidade são introduzidos e tratados naturalmente dentro de um cenário de aquisição gradual de confiança ou de um processo interativo de distribuição dessa confiança adquirida.
Para se verificar a adeqüabilidade e a aplicabilidade dos conceitos introduzidos pelo modelo dinâmico de segurança são especificadas algumas aplicações seguras típicas para o ambiente doméstico. Tais aplicações estão em estágio de implementação já que a análise de seus requisitos mostrou a total aplicabilidade do modelo utilizado.
Uma outra característica associada ao modelo é a sua compatibilidade com o ambiente de programação da linguagem Java e o seu modo atual de tratamento de segurança. A solução proposta deve ser encarado como uma extensão essencial ao modelo de segurança Java para adequa-lo ao ambiente de redes Ad-Hoc.

1 Introdução

Nos últimos anos as redes de computadores tem experimentado um avanço muito intenso. O advento da Internet, originalmente no meio acadêmico, provocou uma corrida acelerada e muito dinâmica, na produção de novas técnicas, mecanismos, protocolos e arquiteturas de comunicação de dados permitindo o aprimoramento e a melhoria em tudo aquilo que tradicionalmente era praticado. Com o início da fase comercial da Internet, essa sucessão de avanços tecnológicos passou também para o campo da comunidade de usuários. O que era simplesmente um meio de comunicação e troca de informações para a comunidade acadêmica passou a servir a sociedade em geral, tanto indivíduos como pessoas jurídicas, com abrangência mundial.

Esta fase de aumento de cobertura e penetração na sociedade mundial, associado a disseminação do uso dos serviços World Wide Web, que constituem a teia mundial de informações, fizeram com que a Internet, e consequentemente, as redes de computadores, deixassem de ser uma simples infra-estrutura de comunicação de dados para se tornar na infra-estrutura indispensável de informações. A teia mundial se tornou algo tão essencial quanto a rede de energia elétrica ou a rede de telefonia para a nossa sociedade.

A presença mundial e a disponibilidade a qualquer tempo da teia da informação nos tem levado naturalmente, ao desejo de operar e receber serviços a partir de qualquer lugar e a qualquer instante. A ubiqüidade das informações e dos serviços passou a ser algo naturalmente desejado e tem permitido se relegar as distâncias que sempre representaram uma condição de contorno restritiva para o inter-relacionamento entre os indivíduos e para a disponibilidade ampla das informações e da prestação de serviços.

Do ponto de vista das comunicações, a Internet se sustenta através de uma rede mundial de computadores estruturada de forma completamente diferente das tradicionais redes de telecomunicações. Ela não possui uma entidade central capaz de controlar e dirigir todas as trocas de mensagens. Em princípio, esta falta de controle central pode parecer algo impeditivo para a operação eficiente de uma infra-estrutura de comunicações. Porém, o que temos observado nos dias de hoje, é que tal infra-estrutura distribuída sem controle central, opera em nível global de forma a viabilizar a existência da teia mundial de informações. Esta questão do gerenciamento eficiente sem uma organização central de administração tem intrigado de forma intensa os projetistas e administradores de redes, e tem sido motivo de grandes debates entre as principais autoridades na operação, na manutenção e na administração de redes de comunicações.

Seguindo as tendências evolutivas da tecnologia de comunicação, mais recentemente, o aparecimento das redes sem fio provocou uma outra onda de avanços que dotou a nossa sociedade de uma capacidade de mobilidade praticamente impensável a alguns anos atrás. As redes móveis também revolucionaram a natureza da infra-estrutura necessária para as comunicações entre indivíduos ou mesmo entre computadores. A implantação e a passagem de cabos de cobre até os extremos das redes de comunicação esta ficando desnecessária. A última milha dessas redes pode ser atendida mais facilmente e com custo bastante

reduzido, comparado ao da estrutura cabeada tradicional, se utilizarmos a tecnologia de comunicação sem fio.
O aparecimento dos telefones celulares evidencia essa evolução onde em quase toda parte do mundo, mas principalmente nos países em que as redes de telecomunicações tradicionais ainda não estavam tão desenvolvidas, a alternativa de cobertura por redes sem fio apareceu como uma solução mais adequada, não só pelo menor custo envolvido como também pela facilidade e agilidade em sua implantação. As redes de comunicação de telefones celulares são infra-estruturadas, ou seja, as estações móveis devem estar em permanente contato direto com uma estação de suporte a mobilidade. Esta estação, por sua vez, esta interconectada de maneira tradicional a uma espinha dorsal de alta velocidade que suporta todas as comunicações da rede móvel sem fio.
Quando pensamos na comunicação de dados móvel sem fio para computadores é bastante conveniente se pensar na situação em que não seja necessário a conexão direta permanente com uma infra-estrutura central. Neste caso, dizemos que essas redes, não estruturadas, são chamadas de redes Ad-Hoc. A ausência de uma infra-estrutura pré-estabelecida faz com que as redes Ad-Hoc apresentem grande versatilidade e facilidade de constituição ou implantação. O conceito de cobertura passa a ter uma característica dinâmica muito mais próxima das necessidades de mobilidade num ambiente onde a ubiqüidade é um fator desejável e indispensável. Nestas redes os equipamentos de infra-estrutura se confundem com os de usuários, sendo que estes podem agir tanto como estações de trabalho ou como elemento intermediário na trajetória para se chegar ao destino final desejado.
Dentro do ambiente da teia mundial, com a capacidade de comunicação sem fio e a conseqüente mobilidade resultante, pode-se imaginar a amplificação do conceito de "a qualquer instante e em qualquer lugar". Agora, para se estar conectado à rede mundial não será necessário que o usuário esteja cabeado fisicamente a um ponto de acesso. A interconexão à teia mundial ou a um ambiente privado local pode ser feita através de redes Ad-Hoc, usando a comunicação sem fio sem a necessidade de um infra-estrutura previamente projetada e implantada. Os usuários nessas redes, terão uma característica mais dinâmica, podendo surgir ou desaparecer da rede por simplesmente saírem ou entrarem no raio de alcance das comunicações sem fio. Um usuário estranho ou um visitante conhecido, pode, em princípio, se conectar á uma rede Ad-Hoc sem que seja necessária uma conexão física a um ponto previamente cabeado. Tal flexibilidade, certamente será responsável pela facilidade de se implantar redes com extrema agilidade e baixo custo em ambientes onde existe a convergência do público atraído por algum evento de grande interesse comum, tal como uma conferência, casa de espetáculo, praça de esportes, hospitais ou mesmo no próprio ambiente doméstico.
De alguma forma, as redes Ad-Hoc podem e devem estar conectadas a alguma espinha dorsal de alta velocidade que permite a integração completa dessa rede sem fio com a infra-estrutura tradicional das redes cabeadas. No contexto das redes de espinha dorsal, as comunicações óticas estão provocando um outro avanço igualmente ou mais importante na capacidade das redes de comunicação de dados. As fibras óticas, já em grande parte lançadas em áreas geográficas de interesse econômico ou estratégico, são capazes de prover uma comunicação de alta capacidade com uma qualidade de serviço adequada aos mais exigentes tipos de

tráfego multimídia. A largura de banda de comunicação praticamente infinita oferecida pelas redes óticas está provocando uma revolução no custo e na qualidade das comunicações. O sonho das comunicações a custo praticamente zero pode se tornar realidade, já que a fonte de receita nessas redes deverá passar para a prestação de serviços e não simplesmente pela disponibilização da comunicação. Este fator de redução de custo acoplado à ubiqüidade da Internet acessada pelas redes móveis sem fio, possui um efeito amplificador na aceleração do desenvolvimento da teia mundial e na sua utilização como meio para a realização de interações pessoais e institucionais de natureza privada ou pública, voltadas para a obtenção de informações ou para transações comerciais, industriais, educacionais, governamentais, financeiras ou de outra natureza qualquer.

1.1 Motivação

O avanço intenso das redes de computadores observado nos últimos anos, principalmente com a mobilidade e ubiqüidade oferecida pelas redes Ad-Hoc, deve intensificar a presença e a necessidade da Internet, a infra-estrutura da informação, na vida diária de nossa sociedade. As relações tradicionais existentes estão sendo repensadas e remodeladas para tirar proveito desse novo ambiente de comunicações. A maneira como a sociedade interage esta sofrendo profundas transformações. Interações entre indivíduos ou entre indivíduos e instituições públicas (governamentais ou não) ou privadas (corporações) ou unicamente entre instituições, não só devem ser reformuladas como também intensificadas. Elas estão abrindo a possibilidade para a prestação de serviços com grande conveniência, tirando proveito da remoção da barreira da distância, e permitindo a disponibilização de informações em larga escala favorecendo a transparência nas relações entre todas as entidades interagentes ou interessadas.

No ambiente governamental, tais características devem ter um efeito muito importante devido a necessidade de transparência pública na condução das ações governamentais perante a sociedade. Ações desta natureza, devem permitir a prestação de serviços públicos com mais eficiência e a baixos custos, para uma parcela cada vez maior da população. Elas devem também minimizar ou dificultar ações fraudulentas ligadas aos bens públicos permitindo que a sociedade acompanhe de maneira eficaz a atuação das instituições governamentais e a conseqüente aplicação dos recursos públicos. A própria democracia deve ser reforçada pela possibilidade de realização de interações entre os representantes do povo e seus eleitores em larga escala e muito rapidamente de uma forma inimaginável há alguns anos atrás.

Nos dias de hoje, já observamos estes efeitos na atuação do governo brasileiro com resultados tão importantes expressos através de nosso sistema de declaração de imposto de renda, do processo de votação eletrônica, ou mesmo dos processo de leilões públicos para aquisição ou vendas de ativos pelo governo. É claro, que estes sistema ainda necessitam de muitas melhorias e aprimoramentos mas é inegável que eles já representam um avanço notável na relação de transparência de informações entre as instituições governamentais e a sociedade.

No ambiente educacional temos observado enormes avanços ou possibilidades de avanços face a evolução das redes de computadores. A disponibilização das redes de alta capacidade permitindo o transporte de tráfego de grande volume com qualidade de serviço compatível com a demanda das mídias contínuas ou discretas, deverá permitir a interação com alta fidelidade a distância. Esta capacidade de interação com alta qualidade se aproximando do potencial interativo disponível no relacionamento presencial, está permitindo que sistemas de educação a distância possam ser concebidos com resultados muito promissores, compatibilizando o ensino de alta qualidade com uma oferta global para uma grande quantidade de alunos.

Certamente, mudanças culturais deverão ocorrer em paralelo às tecnológicas para que estas inovações possam ser utilizadas em sua plenitude. Não basta a tecnologia mudar e avançar, se faz necessário que o homem possa repensar a sua forma da atuação face a esses progressos tecnológicos de maneira tal que ele possa aplicar concientemente e eficazmente essas inovações em prol do bem estar econômico e social da sociedade.

Nas relações comerciais também estão ocorrendo transformações importantes. A condução de negócios on-line já é uma realidade nos dias de hoje. Cada vez mais as corporações estão sentindo a necessidade de integrar as suas operações tradicionais com aquelas que podem ser realizadas através de interações on-line a distância com a utilização da Internet. As empresas e seus clientes, as indústrias e seus fornecedores, as cadeias completas de fornecimento de bens e serviços, as empresas pequenas ou as grandes corporações, o governo ou as instituições não governamentais, enfim todos os segmentos de nossa sociedade estão sentindo a necessidade ou já estão tirando proveito da interação através das redes com o intuito de aprimorar, intensificar, complementar, aumentar a produtividade, reduzir custos ou tornar mais conveniente os serviços prestados e mais eficientes a sua própria operação e administração.

Dentro deste contexto de intensificação das relações e interações on-line através da Internet, envolvendo também, e principalmente, os ambientes de redes sem fio, certas questões merecem maior atenção e cuidado para que os efeitos positivos dos avanços tecnológicos possam realmente ser incorporados como benefícios para a nossa sociedade.

As transações comercias possuem em sua estrutura diversas etapas decisivas durante a execução do processo de comercialização. Estas etapas tradicionalmente são chamadas de etapas de liquidação, pois cada uma delas encerra uma interação específica e conclusiva na comercialização de bens e serviços. A primeira delas é a liquidação comercial, na qual o cliente através de um processo específico de busca e seleção em catálogos eletrônicos escolhe os bens ou serviços a serem adquiridos. Uma vez selecionados os itens desejados, a transação passa para a etapa de liquidação financeira, necessária para a concretização da operação comercial. É através desta etapa que se confirma a transação e se empenham os recursos financeiros atrelados a ela. Somente após a liquidação financeira ou a certeza de que ela irá ocorrer, é que se passa para uma outra etapa que envolve a entrega ou o transporte dos bens ou serviços envolvidos na transação. Esta etapa é a liquidação física da transação comercial, que encerra o ciclo inicial dessa operação.

Todas estas liquidações envolvem a troca de informações sensíveis e que se não forem adequadamente tratadas podem provocar enormes malefícios aos seus

participantes. As transações comerciais envolvem informações ligadas a transferências de recursos e informações de natureza privada que podem revelar aspectos determinantes do comportamento dos indivíduos ou instituições envolvidas na transação. Consequentemente, estas operações devem ser tratadas com o maior sigilo, privacidade, integridade e segurança de uma forma em geral, inclusive procurando-se garantir que as ações executadas em cada uma das etapas sensíveis da transação comercial não possam ser negadas por seus participantes após o término da mesma - característica usualmente conhecida como não repudiação. Estes são requisitos típicos de qualquer sistema que necessita de segurança da informação para que possa atingir com sucesso todos e somente aqueles objetivos previstos pela transação.

Num ambiente onde se realizam transações comerciais envolvendo um número muito grande de participantes que possam se conectar à rede através de um canal de acesso sem fio ou de uma rede Ad-Hoc, as caraterísticas de mobilidade, ubiqüidade e dinamismo determinam uma comunidade incerta e desconhecida de possíveis participantes ou observadores dos fatos e ações pertinentes as transações sendo realizadas. O dinamismo que permite aos usuários estarem presentes ou ausentes, ou que visitantes desejados e conhecidos ou estranhos e indesejados, possam estar em condições de observar ou mesmo tentar participar das transações sendo realizadas, torna este ambiente extremamente desafiador para a garantia da segurança da informação, tão necessária para a consolidação do sucesso e da utilização em larga escala das redes como veículo preferencial para este tipo de transação.

Nos últimos anos, diversas iniciativas de pesquisa enfocando aspectos de segurança nos sistemas on-line tem sido tomadas para que se possa criar um ambiente ao mesmo tempo confiável e flexível para a realização de interações comerciais. Organismos internacionais de padronização tem publicado normas e padrões relativos a mecanismos e protocolos de segurança procurando atender a esta demanda por sistemas transacionais seguros.

A iniciativa da linguagem de programação Java ilustra muito bem uma dessas iniciativas. Esta linguagem foi concebida dentro de um modelo de segurança da informação desde o seu início. O modelo de segurança da linguagem Java procurou tratar as necessidades de interação via redes de computadores onde não só dados são trocados pelos agentes interagentes mas também programas residentes em sites remotos podem ser executados num site local sem que se tenha qualquer risco de violação de privacidade, confidencialidade, integridade ou disponibilidade.

Desde 1995, este modelo de segurança vem sofrendo alterações e complementações visando dotar o ambiente Java Web de recursos capazes de atender a estas demandas de segurança. Em sua versão mais recente, o modelo de segurança Java apresenta recursos bastante importantes para que se alcance um nível bem adequado na segurança dos sistemas de informação implementados em Java. Porém, mesmo com todos estes avanços este modelo ainda não contempla as características dinâmicas inerentes aos ambientes das redes Ad-Hoc.

Portanto, tem-se observado que os modelos de segurança existentes para redes públicas cabeadas (Internet) não levam em conta adequadamente as questões do dinamismo e da presença sempre latente de possíveis intrusos ou de visitantes desejáveis. Mesmo quando estamos tratando de uma rede localizada em um

ambiente privado, porém utilizando o paradigma da comunicação sem fio, o mesmo dinamismo aparece e novamente impacta os cuidados que devem ser tomados relativamente a segurança da informação.
Normalmente, nos sistemas ligados e operados por uma instituição ou corporação, os usuários são primeiramente identificados e autenticados para que depois possam participar de qualquer interação ou transação que envolva informações sensíveis. Para que o usuário, nesse ambiente privado, possa se submeter ao processo de identificação e autenticação, ele deve inicialmente estar conectado fisicamente à rede. Já no contexto de uma rede sem fio, basta que o usuário esteja dentro do raio de alcance das comunicações locais para que ele possa tentar interferir ou simplesmente observar as transações em curso. Neste caso, a vulnerabilidade do sistema se torna muito mais acentuada e cuidados adicionais devem ser tomados para que não se tenha uma interferência negativa impossibilitando a aplicação, extremamente conveniente, dessas redes sem fio para multiplicar o uso das interações entre os agentes participantes.
Não basta tentar impedir a presença dos elementos visitantes, sejam eles conhecidos ou não, para que se tenha um ambiente seguro. Em situações onde ocorrem grande afluência de público atraído por algum interesse comum, tais como, em casas de espetáculo, praças esportivas, campus educacionais, hospitais etc., o elemento não conhecido é o nosso cliente e é exatamente ele que deve participar da transação sensível. Nestes casos, é natural que a relação de confiança existente entre os elementos participantes da transação seja variável no tempo e não obedeça a uma relação previamente estabelecida e constante ao longo do tempo, com acontece nas situações de redes públicas ou privadas cabeadas. Esta variação temporal nas relações de confiança interfere no modelo de segurança necessário para a condução adequada das transações comerciais em ambientes Ad-Hoc.
Se novos modelos de segurança, que incorporem estes efeitos de variação temporal, não forem desenvolvidos estaremos diante de um fato extremamente limitador ao aumento do uso das redes, principalmente da Internet com aceso sem fio. Para que possamos tirar proveito de todos os benefícios proporcionados pelos avanços tecnológicos nos últimos anos ocorridos na área de redes de computadores sem fio é imperativo que novos modelos de segurança sejam pesquisados e desenvolvidos.
Dentro deste cenário é que posicionamos este trabalho que objetiva a definição de um modelo de segurança para redes Ad-Hoc que contemple variações temporais naturais nas relações de confiança entre seus participantes. Associado a este modelo deve se definir uma arquitetura de segurança que identifica todos as entidades, relacionamentos, mecanismos, protocolos e serviços necessários para se constituir um ambiente seguro para redes Ad-Hoc. A materialização dessa arquitetura de segurança e a conseqüente evidência de viabilidade se dá através da definição de um "framework" para desenvolvimento de aplicações seguras em ambiente de redes Ad-Hoc.

1.2 Organização do trabalho

Este trabalho está organizado em 7 capítulos. O primeiro deles, que é esta introdução, apresenta o cenário onde se posiciona e se desenrola o trabalho

identificando os fatores que sustentam as motivações que levaram a definição do tema desta pesquisa.
O capítulo 2 apresenta uma breve introdução as redes Ad-Hoc focando em algumas definições e exemplos das duas tecnologias que tem sido mais utilizadas: uma para o ambiente de interconexão de equipamentos e outra para a constituição de redes locais sem fio.
O capítulo 3 apresenta algumas definições ligadas a segurança da informação e discute aspectos importantes da segurança em redes Ad-Hoc e seus correspondentes mecanismos que determinam o substrato onde estará apoiado todo o modelo de segurança proposto neste trabalho.
O capítulo 4 apresenta a formalização do modelo de segurança para redes Ad-Hoc lidando com o dinamismo natural deste ambiente e formulando mecanismos que possam tratar adequadamente a variação temporal das relações de confiança entre os seus elementos participantes. Este capítulo apresenta a contribuição mais importante deste trabalho.
O capítulo 5 descreve a arquitetura associada ao modelo de segurança para redes Ad_Hoc apresentado no capítulo anterior. A definição da arquitetura não é completa , mas o suficiente para se demonstrar a sua viabilidade e exeqüibilidade face aos conceitos e características definidas pelo modelo de segurança.
O capítulo 6 materializa a arquitetura do modelo de segurança através da formulação dos requisitos básicos para o desenvolvimento de aplicações seguras em redes Ad-Hoc. A caracterização completa e o desenvolvimento da aplicação mencionada neste capítulo é tema de outros trabalhos no âmbito de mestrado e doutorado orientados pelo autor.
O capítulo 7 encerra as conclusões finais do trabalho apontando para outros documentos e dissertações que estão sendo realizados e que certamente complementarão os resultados aqui apresentados.

2 Redes Ad hoc: Definições e Tecnologia

2.1 Definições

Uma rede ad hoc é definida como um conjunto de nós ou plataformas móveis que podem se deslocar arbitrariamente em uma infra-estrutura temporária e estabelecer uma rede efêmera de comunicação sem a presença de uma entidade central.
Nos últimos anos, assistiu-se a um rápido crescimento no desenvolvimento de redes experimentais com transmissão via rádio. Contudo, o IEEE definiu um padrão (IEEE 802.11) para redes locais sem fio (WLAN) em que os pacotes são trocados via rádio. De acordo com esse padrão, as redes sem fio podem ser classificadas como independentes (ad hoc) ou com infra-estruturadas [CALO00].
Em uma rede infra-estruturada, os nós móveis (MH) estão conectados por meio de uma conexão sem fio a uma estação de apoio a mobilidade (MSS); a MSS possibilita a conexão do MH a uma rede com fio. Nesse tipo de rede sem fio, todas as comunicações necessitam ser feitas por meio do MSS. A MSS define uma área onde

ela possa ser alcançada por um MH. Para se obter um alcance maior, várias MSSs devem ser utilizadas, como mostra a Figura 1.

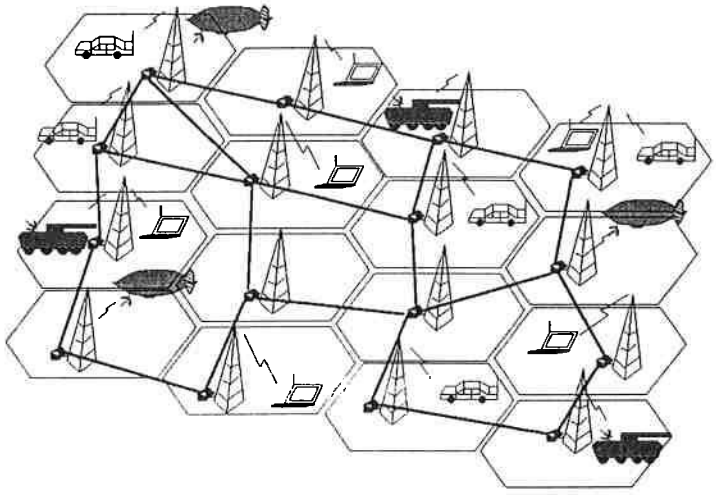


Figura 1: rede móvel com infra-estrutura [CALO 00]

Uma rede móvel ad hoc é uma rede formada sem administração central: os nós móveis usam uma interface sem fio para mandar pacotes de dados. Os nós nesse tipo de rede podem atuar como servidores (executando aplicações de usuários) e como roteadores (encaminhando pacotes para outros nós, para estender o alcance da rede). Em uma rede ad hoc (MANET – Rede móvel ad hoc), os equipamentos são capazes de trocar informações entre si, como mostra a Figura 2.

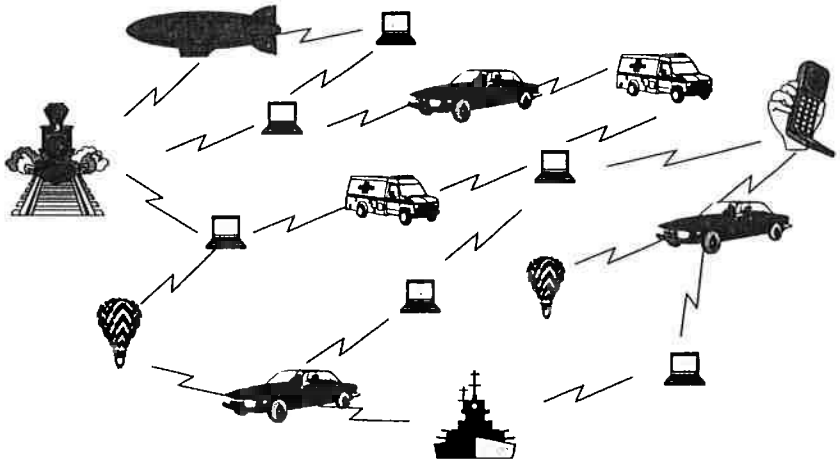


Figura 2: redes móveis ad hoc

2.1.1 Modo de operação

A operação de uma rede ad hoc pode ser classificada como de passo único ou de passos múltiplos.

- Passo único: dois dispositivos só se comunicam diretamente. Eles precisam estar ao alcance um do outro, o que pode limitar a comunicação

somente a curtas distâncias. Por outro lado, não há necessidade de roteamento;

- Passos Múltiplos: dois dispositivos com uma grande distância entre si (fora de alcance) comunicam-se indiretamente: na MANET, a comunicação entre dois dispositivos pode ser executada através de múltiplos passos, percorrendo um ou mais nós da rede, os quais atuam, neste caso, também como roteadores.

Os problemas fundamentais em uma rede ad hoc são:

- a determinação e a manutenção das rotas entre os dispositivos, já que a mobilidade de um computador pode modificar a topologia e, por conseqüência, as rotas; e
- a segurança das informações, dispositivos e serviços que operam nesse ambiente.

2.1.2 Aplicações típicas

As redes ad hoc podem ser preferencialmente utilizadas em situações em que não haja infra-estrutura de comunicação previamente disponível. Os dispositivos de usuário podem ser interconectados entre si e também a um ponto local de informação. Além disso, as redes ad hoc são adaptadas para situações em que não é possível instalar uma rede com fio, como, por exemplo, em operações de resgate ou na conexão de edifícios urbanos afastados.
Em ambiente doméstico, as redes ad hoc que podem conectar *notebooks, palmtops* ou mesmo a outros dispositivos tipicamente caseiros, tais como Televisor, refrigerador, aparelho de ar condicionado, etc. Uma vez conectados eles podem ser usados para se comunicar, divulgar e compartilhar informações (como por exemplo informações de áudio/vídeo) entre parceiros compatíveis.

Tipicamente, em curtas distâncias, as redes ad hoc podem conectar muitos dispositivos móveis, sem a necessidade dos cabos físicos, obtendo-se assim uma rede personalizada (PAN).

2.1.3 Vantagens e desvantagens

Entre as vantagens das redes ad hoc, podemos citar [PERK 01]:

- Instalação rápida: sem necessidade de infra-estrutura, redes ad hoc podem ser instaladas de modo fácil e rápido.

- Tolerância a falhas: problemas em um nó de roteamento podem ser reparados por meio de uma reconfiguração dinâmica da topologia da rede;
- Conectividade: se dois dispositivos estão dentro do alcance de ondas de rádio, a conexão é mantida;
- Mobilidade: dentro de uma área de alcance, os dispositivos podem mudar de lugar em qualquer momento.

Existem também desvantagens associadas as redes ad hoc, tais como:

- Banda estreita: normalmente as conexões sem fio têm uma banda de comunicação menor que as conexões com fio;
- Maiores taxas de erro: como as conexões sem fio são mais suscetíveis a interferências, normalmente elas têm maiores taxas de erro;
- Localização: é um problema encontrar a localização de um usuário ou serviço, já que não há nenhuma informação geográfica sobre o nó sem fio e o endereço do nó não tem nenhuma relação com o lugar em que o nó se encontra;
- Roteamento: o nó se move de um lado para o outro, de uma maneira não determinístico, formando uma topologia dinâmica e, como conseqüência, tabelas de roteamento também dinâmicas.
- Segurança: qualquer dispositivo capaz de emitir um sinal de rádio pode tentar entrar na rede, fazendo com que a segurança seja um dos assuntos mais importantes a serem tratados em tais sistemas.

2.1.4 Características e Requisitos

Uma rede ad hoc opera num ambiente em que todos os nós são móveis. Neste ambiente dinâmico, a funcionalidade da rede deve ser executada num cenário distribuído, com as seguintes características:

- Operação Distribuída: um nó confia na rede (isto é, pode trocar informações sensíveis com nós confiáveis) se ela tiver uma política de segurança e uma funcionalidade adequada para operar de maneira distribuída.
- Topologia Dinâmica da Rede: geralmente, os nós são móveis, o que resultará numa topologia de rede variável. Contudo, a conectividade da rede não deve ser

interrompida por causa disso, a fim de permitir a operação contínua de serviços e aplicações;

- Banda de comunicação variável: os efeitos da taxa de erro em conexões de múltiplos passos em redes ad hoc é potencialmente maior. Se uma conexão for quebrada, muitas seções serão interrompidas, ocasionando uma alta taxa de ocorrência de erros na transmissão. Neste caso, as funções de roteamento estarão comprometidas.

2.2 Tecnologias da rede AD HOC

Presentemente, existem duas tecnologias capazes de suportar uma rede AD HOC: a IEEE 802.11 e Bluetooth. A primeira é mais velha e permite distâncias maiores, sendo usada principalmente para implantar rede locais (LAN). A segunda é mais adequada para compor pequenas redes com dispositivos mais próximos. Esta seção explica sucintamente as principais características destas duas tecnologias.

2.2.1 IEEE 802.11

2.2.1.1 Introdução

Redes sem fio têm características diferentes das redes com fio. Baseado nessas características, o padrão IEEE 802.11 [802.11] define conceitos e componentes da arquitetura usados para representar implementações físicas específicas de redes locais sem fio (WLAN).

O padrão IEEE 802.11 inicial, que é oficialmente chamado de "Padrão IEEE para Especificações da Camada de Acesso ao Meio LAN Sem Fio (MAC) e Camada Física (PHY)", define os protocolos necessários para suportar uma rede local. Como com outros padrões IEEE 802 (por exemplo, 802.3 e 802.5), o serviço primário do padrão 802.11 é o de entrega de MSDUs (MAC Service Data Units) entre pares LLC (Logical Link Control). Tipicamente, uma placa de rede sem fio e um ponto de acesso provêem as funções do padrão IEEE 802.11 [802.11].

2.2.1.2 Características

O padrão IEEE 802.11 oferece funcionalidade MAC e PHY para conectividade sem fio de estações fixas, portáteis ou móveis, movendo-se em velocidade de pedestres ou veículos dentro da área local. O padrão IEEE 802.11 inclui as seguintes características específicas:

- Suporte a serviço de entrega assíncrono e limitado por tempo;
- Continuidade do serviço dentro de áreas estendidas através de um Sistema de Distribuição, tal como Ethernet;
- Acomodação de taxas de transmissão de 1Mbps (opcional 2Mbps), nas versões mais atuais velocidades mais rápidas são alcançadas;
- Suporte a maioria das aplicações de mercado;

- Serviços de Multicast (incluindo broadcast),
- Serviço de gerenciamento de rede;
- Serviço de registro e autenticação.

A utilização deste padrão se aplica aos seguintes ambientes:

- Interior de edifícios, tais como, escritórios, bancos, lojas, shopping centers, hospitais, fábricas e residências
- Áreas externas, tais como estacionamentos, campi de universidades, praças esportivas, complexos de edifícios e fábricas externas.

O padrão 802.11leva em conta as seguintes diferenças significativas entre LANs sem fio e com fio:

- Gerenciamento de energia: Devido ao fato da maioria das placas de rede para redes locais sem fio estarem disponíveis em formato PCMCIA Tipo II, é possível capacitar equipamentos portáteis com conectividade sem fio. O problema, contudo, é que esses dispositivos precisam contar com baterias para acionar seus componentes eletrônicos internos. O acréscimo de um LAN NIC sem fio a um computador portátil pode rapidamente descarregar as baterias. A camada MAC implementa as funções de gerenciamento de energia colocando o rádio em estado de espera (isto é, baixando o consumo de energia) quando não há atividade de transmissão acontecendo por alguma razão específica ou por uma definição de tempo do usuário. O problema, contudo, é que uma estação em estado de espera pode perder transmissão de dados importantes. O padrão IEEE 802.11 resolve este problema criando *buffers* para a fila de mensagens. O padrão determina o acionamento periódico de estações em estado de espera, para recuperar quaisquer mensagens pertinentes.
- Largura de banda: A faixa de freqüencias ISM não oferecem muita largura de banda, mantendo as taxas de dados mais baixas que o desejável em algumas aplicações. Para lidar com este problema, o grupo de trabalho do IEEE 802.11, contudo, especificou métodos para compressão de dados (por exemplo, BPSK para largura de faixa de 1Mbps e QPSK para 2Mbps), tentando minimizar as restrições impostas pela largura de banda disponível.
- Segurança: LANs sem fio transmitem sinais em áreas muito maiores que aquelas com meios com fio, tais como cabo de par trançado, cabo coaxial e fibra ótica. Quanto à privacidade, contudo, LANs sem fio têm uma área muito maior para proteger a privacidade das comunicações. Para garantir a segurança, o IEEE 802.11 tem um grupo de trabalho especial, o IEEE 802.11i WG, responsável pelo desenvolvimento de mecanismos de segurança.
- Endereçamento: A topologia de uma rede sem fio é dinâmica; portanto, o endereço de destino nem sempre corresponde ao local de destino. Isso gera um problema quando pacotes são roteados através da rede para o destino desejado. Dessa forma, pode-se precisar usar como o MobileIP, para suportar estações móveis.

2.2.1.3 *Componentes*

A topologia do IEEE 802.11 consiste de componentes que permitem a mobilidade da estação transparente as camadas mais altas de protocolos, tais como LLC. Uma estação é qualquer dispositivo que contenha a funcionalidade do protocolo IEEE 802.11 (isto é, camada MAC, camada PHY e interface para um meio sem fio). As funções do padrão IEEE 802.11 consistem de uma placa de rede sem fio, a interface de software que controla a mesma, e um ponto de acesso. O padrão IEEE 802.11 suporta três topologias:

- Basic Service Set (BSS);
- Independent Basic Service Set (IBSS);
- Extended Service Set (ESS).

Essas redes usam um módulo básico, referido no padrão IEEE 802.11 como um BSS, oferecendo um área de cobertura onde estações de BSS permanecem totalmente conectadas. Uma estação é livre para se mover dentro da BSS, mas não pode mais se comunicar diretamente com outras estações se ela deixa o BSS. Uma estação endereçável especial na rede, chamada de ponto de acesso (AP), controla as transmissões dentro do BSS e pode fornecer conexão entre o BSS e uma rede com fio (Figura 3).

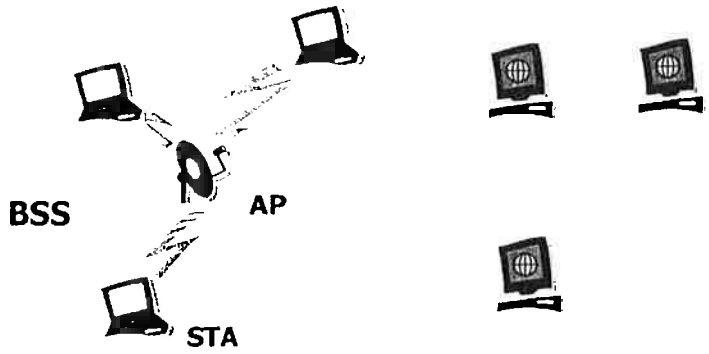


Figura 3: Topologia IEEE 802.11 BSS

É também possível definir uma rede sem ponto de acesso, onde as estações se comunicam diretamente entre elas, se elas estão dentro do alcance. Esse tipo de rede é uma rede IBSS (Figura 4)

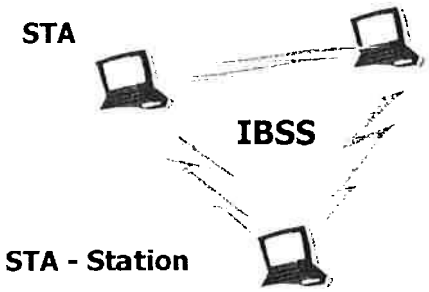


Figura 4: Topologia IEEE 802.11 IBSS

Uma rede ESS é formada pela conexão de diferentes BSSs. O padrão IEEE 802.11 define o *sistema de distribuição* como um elemento que interconecta BSSs dentro do ESS via pontos de acesso. O sistema de distribuição suporta os tipos de mobilidade IEEE 802.11 oferecendo serviços lógicos necessários para lidar com mapeamento de endereço lógico para o dispositivo desejado e integração transparente de múltiplos BSS. (Figura 5).

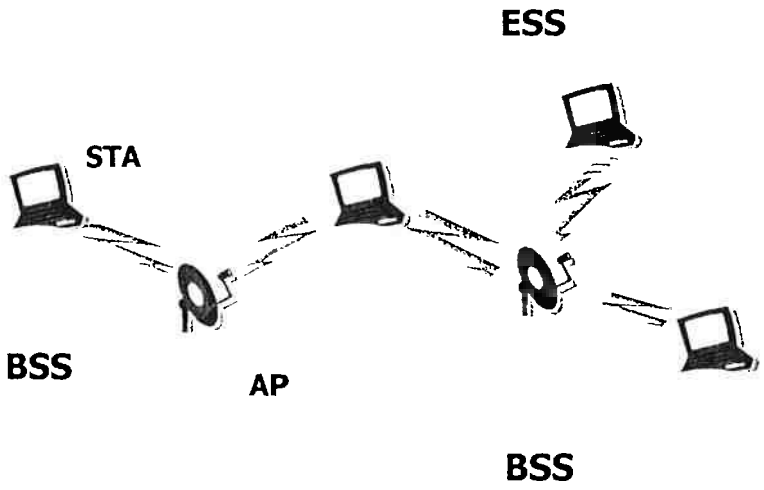


Figura 5: Topologia IEEE 802.11 ESS

O padrão IEEE 802.11 não limita a composição do sistema de distribuição; portanto, pode ser compatível com o 802 ou com alguma rede não padronizada. Se pacotes de dados precisam de transmissão para e a partir de uma LAN que não seja IEEE 802.11, então esses pacotes, como definidos pelo padrão 802.11, entram e saem por um ponto lógico chamado de *portal*. O portal oferece integração lógica entre LANs com fio existentes e LANs 802.11. Quando o sistema de distribuição é construído com componentes do tipo 802, tais como IEEE 802.3 (Ethernet) ou IEEE 802.5 (Token Ring), então o portal e o ponto de acesso tornam-se um só e iguais.

A topologia dessas redes (a BSS, IBSS e ESS) são transparentes para a camada LLC.

2.2.1.4 Arquitetura Lógica

Enquanto a topologia oferece os meios de especificar a estrutura de interconexão dos componentes físicos necessários a uma rede, a arquitetura lógica define a operação da rede. A arquitetura lógica do padrão 802.11 que se aplica a cada estação consiste de um único MAC e um entre diversos PHYs, tais como espalhamento espectral do tipo salto de freqüência (frequency hopping), do tipo seqüência direta (direct sequence) ou luz infravermelha.

O objetivo da camada MAC é oferecer funções de controle de acesso (tais como endereçamento, coordenação de acesso, geração de uma seqüência para quadros de verificação e verificação e delimitação de LLC PDU) para PHYs de meio compartilhados para suportar a Camada LLC. A camada MAC executa o endereçamento e reconhecimento de quadros. O padrão IEEE 802.11 usa um algoritmo chamado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance); similar ao algoritmo usado no padrão Ethernet (CSMA/CD - Carrier Sense Multiple Access with Collision Detection). Não é possível transmitir e receber no mesmo canal ao mesmo tempo usando transceptores de radio; portanto, uma LAN 802.11 sem fio somente toma medidas para evitar colisões (CA), não para detê-las (CD).

2.2.1.5 IEEE 802.11b

O padrão IEEE 802.11b [802.11b] é um aperfeiçoamento do padrão IEEE 802.11 para enlaces de alta velocidade utilizando espalhamento espectral do tipo direct sequence. É possível ter uma largura de banda de no máximo 11Mbps dentro de um alcance de 18 metros (alcance interno), caindo para 5.5Mbps (36 metros) e depois para 2Mbps e finalmente, para 1Mbps.

2.2.2 Bluetooth

A tecnologia Bluetooth foi desenvolvida com o objetivo de eliminar a necessidade de utilização de cabos para interconectar equipamentos eletrônicos e ainda assim, permitir a formação de redes ad hoc. Todas as interfaces entre equipamentos podem ser feitas através de conexão de radio de baixa potência. Dispositivos portáteis, tais como PDAs e telefones celulares podem automaticamente reconhecer um ao outro e trocar dados. A fim de atender às exigências de baixo consumo de energia de dispositivos que funcionam a bateria, o padrão Bluetooth define três classes de potência, com crescente consumo de energia e cobrindo faixas maiores: 1mW, 2,5mW e 100mW, que estão dentro de 10m, 20m e 100m de área de alcance respectivamente [BLUE01A].

2.2.2.1 *Componentes*

Uma rede Bluetooth é chamada de piconet e pode ter até oito dispositivos ativos. Estes dispositivos são classificados como dispositivos master ou slave, dependendo da função deles na rede [BLUE01A] [BRAY01].

Um piconet é formado por um conjunto de slaves unidos por um master. O master é o dispositivo que inicia a conexão com outro dispositivo, chamado de slave. Os slaves são conectados somente ao master e até sete slaves podem estar ativos numa piconet. A Figura 6 mostra um exemplo de uma piconet. A circunferência mostra o limite da piconet, na qual qualquer dispositivo dentro dessa área pode fazer parte desta piconet.

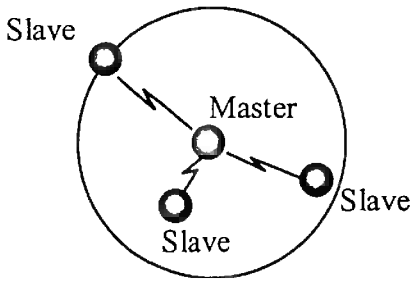


Figura 6: Piconet

O master tem as seguintes funções:

- Controla quando os aparelhos estão habilitados a transmitir;
- Faz a alocação de intervalos de tempo (slots) para tráfico de voz e dados para os slaves transmitirem;
- Controla a distribuição da largura de banda total disponível entre os slaves. O sistema de distribuição em intervalos de tempo (time slots) entre dispositivos múltiplos é chamado de TDD (Time Division Duplex).

Os slaves devem obedecer às seguintes regras quando são parte de uma piconet:

- Todos os dispositivos slaves são sincronizados com o FH[1] do master.
- Um slave somente se conecta a um dispositivo master.

Piconets podem ser agrupadas, formando um rede espalhada (scatternet), onde alguns dispositivos podem ser parte de um ou mais piconets. A Figura 7 mostra um dispositivo sendo parte de uma piconet como slave e formando outra piconet como master.

[1] FH (Frequency Hop): seqüência dos saltos de freqüência utilizada pela técnica de espalhamento espectral, FHSS.

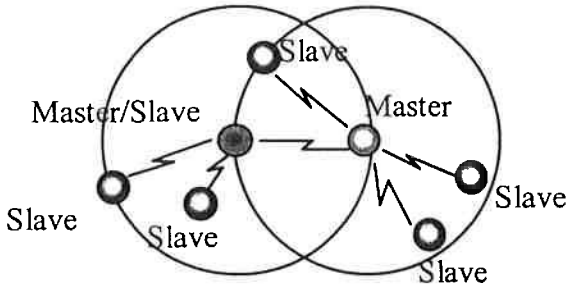


Figura 7: Scatternet com um dispositivo sendo slave de uma piconet e master de outra

Outra possibilidade é um dispositivo ser parte de duas piconets como slave de ambos, como mostrado na Figura 8.

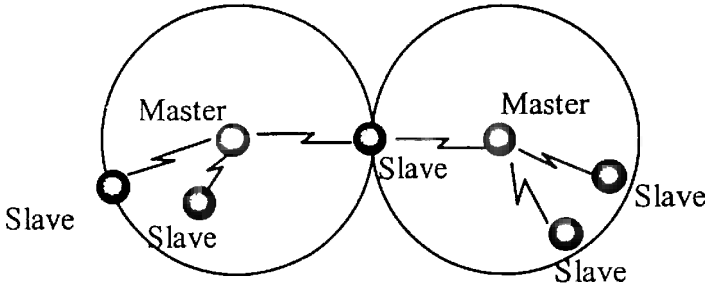


Figura 8: Scatternet com um dispositivo sendo slave de duas piconets

Scatternets são inerentemente mais complexas que uma simples piconet, e eles devem lidar com certas questões específicas. Todos os slaves são sincronizados com o FH do master numa piconet, que gerencia o uso do meio. Mas numa scatternet, por haver mais que um master, o FH nas duas piconets não são sincronizados e colisões aleatórias podem ocorrer na mesma freqüência. Neste caso, os pacotes de dados são retransmitidos e os pacotes de voz são descartados. Quando há muitas piconets a probabilidade de colisão aumenta.

2.2.2.2 Transmissão

A tecnologia Bluetooth trabalha dentro de uma faixa de freqüências que vai de 2.4GHz a 2.438GHz, que é alocada para uso geral por aplicações industriais, médicas e científicas. Estas aplicações devem atender às exigências relativas ao nível de energia, emissão de espectro e interferência. A técnica de espalhamento espectral do tipo salto de freqüência (frequency hopping) (FHSS) é utilizada e toda a largura de banda é dividida em canais de 1MHz. A comunicação dentro de uma piconet é feita alternando-se entre canais de transmissão na mesma seqüência master (dispositivos Bluetooth saltam a uma taxa de 1600 saltos/s). Se há interferência em um canal, a próxima transmissão ocorre num canal diferente.

Como se vê, uma freqüência de salto deve ser definida de modo que dois dispositivos possam estabelecer um canal de comunicação físico. A freqüência de salto é definida pelo dispositivo master: quando dispositivos slaves se conectam ao master eles recebem o endereço e sincronizador do master e, baseado nessas informações, eles geram a seqüência de saltos de freqüência para ser usada na comunicação com o master. Esta seqüência de saltos pseudo-aleatória através de canais de freqüência de rádio (RF) é chamada de canal físico.

A piconet é, então, definida pelo conjunto de dispositivos sincronizados por uma única seqüência de saltos.

2.2.2.3 Estabelecimento da conexão

Bluetooth define uma seqüência de passos para estabelecer uma conexão. Primeiro, um canal precisa ser estabelecido, depois uma conexão física é estabelecida. Só depois do estabelecimento da conexão física o canal lógico pode ser solicitado. A conexão entre aplicações deve ser estabelecida num canal lógico [BLUE01B].

Quando um dispositivo quer descobrir quais dispositivos Bluetooth estão dentro do seu raio de alcance, ele executa um processo denominado "inquiry".

Neste processo, ele transmite uma mensagem de inquiry em diferentes freqüências. Os dispositivos podem varrer essas freqüências procurando por pacotes de pesquisa e, quando encontrados, eles respondem à pesquisa com a informação necessária para o estabelecimento do canal físico (tais como os endereços e sincronizadores dos dispositivos, para conexão e sincronização dos saltos de freqüência).

Após a pesquisa, o dispositivo tem uma lista de dispositivos Bluetooth vizinhos. Depois de selecionar um dispositivo para se comunicar é necessário verificar se ele suporta o serviço específico desejado. Neste processo, denominado paging, o dispositivo selecionado responde com todas as informações necessárias sobre o uso do serviço.

Quando o processo de paging termina, uma conexão física entre os dois dispositivos Bluetooth está estabelecida. Sobre esta conexão, deve-se estabelecer uma nova conexão lógica, chamada de canal lógico. Negociações de segurança podem ocorrer durante ou depois do estabelecimento do canal lógico, dependendo do modo de segurança do dispositivo.

O estabelecimento de uma conexão entre aplicações só é possível depois que um canal lógico é estabelecido. O estabelecimento de uma segunda conexão pode ser feita no mesmo canal lógico, em outro canal na mesma conexão física ou em uma segunda conexão física.

Um dispositivo pode restringir esse acesso inicial de diversas maneiras. Pode estar num modo oculto, quando ele não responde ao processo de pesquisa (e outros dispositivos não o "vêem") ou ele pode estar num modo não conectável, quando ele não responde ao processo de paging.

3 Segurança em redes sem fio: definições, características e mecanismos

3.1 Definições de segurança

Este documento utiliza a classificação [STAL98], que caracteriza os tipos de ataques, serviços e mecanismos relativos à segurança.

Segurança Computacional é a capacidade de impedir que atacantes atinjam seus objetivos através de acesso ou uso não autorizado de computadores ou redes de computadores [HOWA97].

Confiança Computacional é a característica que faz com que alguém confie em um computador e seu software, porque ele se comporta conforme esperado.

Modelo de Segurança e Confiança: é composto por um grupo de entidades, lógicas e físicas, e suas relações relativas aos direitos de acesso, uso legítimo, identificação positiva e confiança, com o propósito de estabelecer um ambiente para comunicação e processamento seguro e confiável.

Arquitetura de Segurança: identifica os componentes de um sistema (computador e suas respectivas redes de comunicação) que são responsáveis por fornecer suporte para implementação das entidades e as suas respectivas relações de segurança e confiança, através de mecanismos e protocolos que garantam direitos de acesso, uso legítimo de serviços, identificação positiva e confidencialidade entre essas entidades.

Framework da aplicação de segurança: é um padrão ("Template") genérico que define a estrutura de uma aplicação segura, baseada em componentes básicos especiais capazes de implementar os mecanismos e protocolos de segurança e confiança necessários a arquitetura de segurança. Este framework poderá ser personalizado através do acréscimo de componentes e funções específicas, tornando-se, então, uma aplicação capaz de fornecer um dado serviço com segurança.

3.2 Ataques

Um ataque é qualquer ação que compromete a segurança das informações, bens ou serviços de propriedade de uma organização. Os ataques podem ser classificados por suas funções, em quatro categorias gerais.

- Interrupção: Ocorre quando o acesso a algum serviço é destruído, indisponibilizado ou inabilitado. Este é um ataque na disponibilidade;
- Interceptação: Ocorre quando um indivíduo, não autorizado, obtém acesso a determinada informação sensível. Este é um ataque na confidencialidade;
- Modificação: Ocorre quando um indivíduo sem autorização não apenas tem acesso a determinada informação como pode, também, alterá-la. Este é um ataque na integridade e confidencialidade da informação;
- Fabricação: Ocorre quando um indivíduo sem autorização insere informações falsas na rede. Este é um ataque de autenticidade.

3.3 Serviços

Falha na segurança é a violação de um ou mais dos seguintes aspectos de segurança relativos à comunicação entre dois ou mais usuários autorizados: confidencialidade, integridade, disponibilidade ou autenticidade.

Confidencialidade é a proteção da *exposição* da informação a indivíduos não autorizados, garantindo a proteção a ataques passivos, tais como análises de tráfego de informações.

Integridade é a garantia da consistência da informação, evitando a criação, modificação ou destruição da informação por terceiro não autorizado. Protege a informação contra a interrupção, fabricação ou modificação de dados.

Disponibilidade significa que usuários legítimos e autorizados não sejam privados de acesso a informações do sistema e/ou recursos.

Autenticidade significa que os recursos não serão utilizadas por indivíduos não autorizados, ou para fins não autorizados.

3.4 Mecanismos

Os mecanismos de segurança são projetados para detectar, evitar ou recuperar informações sujeitas a um ataque à segurança. Um serviço de segurança faz uso de um ou mais mecanismos de segurança ao ser implementado. Os mecanismos usados dependem da tecnologia e serviço de cada rede.

Exemplos de mecanismos de segurança são: criptografia, protocolos de segurança, funções hash, assinatura digital etc.

3.5 Aspectos de segurança em redes Ad-Hoc

A comunicação sem fio tem diversas características que a distinguem dos ambientes tradicionais de comunicação com fio; a maior parte destas estão relacionadas à natureza da comunicação em si. Os sinais de comunicação sem fio *viajam* pelo ambiente, ao contrario da comunicação por fios, onde o sinal é confinado a um fio de cobre ou fibra ótica. Além disso, uma das grandes vantagens do sistema sem fio, a mobilidade do nó, pode levar este a sérios problemas de segurança. As características da comunicação sem fio que podem gerar problemas de segurança se constituem no principal aspecto a ser discutido neste documento.

É importante entender que a comunicação sem fio só pode causar impactos nas camadas física, de enlace ou de rede do modelo OSI. Para a camada de transporte e as camadas acima, este é transparente, o que significa que não interferem na sua funcionalidade. Todos os métodos de criptografia, em especial, utilizados nas camadas de transporte e camadas superiores permanecem válidos.

3.6 Transmissão Física

Nas redes com fio algumas precauções são tomadas para evitar que indivíduos não autorizados tenham acesso à rede. Os dispositivos são fisicamente protegidos contra acesso não autorizado e o cabeamento é protegido contra mecanismos de

captura de dados. Firewalls são instalados para evitar o acesso de nós não autorizados a serviços controlados. Este aspecto importante de segurança pode estar nos pontos de acesso à rede, simplificando a segurança nas aplicações.

Em redes sem fios, não é possível evitar que dispositivos não autorizados tenham acesso à rede. Qualquer dispositivo dentro do alcance dos sinais de freqüência de rádio pode ter acesso aos dados que estejam sendo transmitido, bem como transmitir dados aos dispositivos. Desta forma, ataques de interrupção ou interceptação são mais facilmente realizados em redes sem fio do que em redes tradicionais com fio. Para evitar este tipo de ataque é necessária a implementação de serviços capazes de assegurar a disponibilidade de conexão e a confidencialidade de informações.

Os mecanismos físicos comumente utilizados para dificultar que sinais transmitidos sejam interceptados são as técnicas de espalhamento espectral com baixo potência de transmissão. Esta técnica aumenta a dificuldade para a interrupção de sinais (ex., um ataque do tipo jamming) bem como a interceptação de sinal (evitando a captura de dados da rede).

3.7 Acesso Não Autorizado à Rede e Informações

Algumas características das redes ad hoc podem necessitar de diferentes soluções para segurança. Por exemplo, redes com ou sem ponto de acesso e redes públicas ou privadas requerem diferentes níveis de segurança e as soluções podem ser distintas. Estes quatro tipos de rede são utilizados a seguir, como exemplos de problemas de segurança em redes ad hoc.

3.7.1 Rede Privada

Numa rede de acesso privado, os dispositivos com conexão autorizada são conhecidos e controlados. Estas redes são geralmente criadas para servir um grupo limitado de usuários e dispositivos, tais como:

- Redes de Negócios;
- Redes Domésticas;
- Redes para Automação Industrial;
- Redes criadas para conferências ou reuniões em espaço outro que o ambiente de negócios;
- Provedor de acesso sem fio à Internet etc.

Nestas redes somente dispositivos autorizados podem utilizar a rede, mas nas redes sem fio este controle não é tão simples, uma vez que qualquer pessoa pode transmitir e obter informações no ar. Para manter o controle da comunicação e evitar intrusos os dispositivos precisam ser autenticados reciprocamente.

Nas redes sem fio, todos os dispositivos estão igualmente sujeitos a ataques e, apesar da necessidade do serviço de autenticação dos dispositivos, este serviço pode não ser suficiente para controlar o acesso à rede. Por exemplo, se todos os dispositivos autenticados são considerados confiáveis, quando um dispositivo autenticado é controlado por um intruso, apesar de autenticado, o dispositivo não

pode ser considerado confiável. Cada dispositivo deve prover o controle de acesso aos serviços e a ele próprio.

Outra questão comum nestas redes é a confidencialidade de dados em transmissão. O uso de criptografia é necessário para dados críticos porque não é possível evitar totalmente que um intruso capture o sinal transmitido pelo ar.

3.7.2 Rede Pública

Os serviços públicos da rede podem ser acessados por dispositivos desconhecidos. Esta rede é geralmente criada para usuários itinerantes (provedores de serviços). Alguns exemplos:

- Serviços de Informações oferecidos, por exemplo, em um aeroporto;
- Redes temporárias com pontos de acesso à Internet, criadas para eventos;
- Rede ad hoc Pública: rede criada sem a presença de pontos específicos ou roteadores.

Este tipo de rede pode, ou não, requisitar a autenticação de dispositivos e usuários. Da mesma forma, os dados transmitidos podem ser confidenciais ou não. Geralmente, a necessidade de autenticação e criptografia depende do tipo de serviço. Serviços, por exemplo, como a troca de Cartões de Visita Virtuais e a Locação de Serviços necessitam ser simples e livres do processo de autenticação.

Neste caso os usuários e dispositivos são desconhecidos, o que torna difícil a implementação de mecanismos de criptografia e autenticação, se não impossível. O uso do esquema de chave pública e privada pode oferecer autenticação em nível de aplicação.

3.7.3 Redes Sem Pontos de Acesso

Podem ser redes sem fio isoladas, sem conexão com outras redes. Alguns dispositivos podem ser conectados à outra rede, mas não atuam como gateways ou roteadores. Alguns exemplos:

- Rede de Automação Doméstica e de computadores, quando não conectada à Internet;
- Serviços de rede em aeroportos.

Os problemas de segurança nestas redes são limitados aos dispositivos e serviços locais. Uma falha não se propaga a outras redes. A segurança está somente em cada dispositivo e serviço.

3.7.4 Redes Com Pontos de Acesso

Neste caso um ou mais dispositivos sem fio fornecem um ponto de acesso para a conexão com outras redes. Alguns exemplos:

- Provedor sem fio de acesso à Internet;
- Rede criada em eventos, para acesso à Internet;
- Rede Local sem fio conectada a rede com fio.

Estas redes são conectadas com outras redes, geralmente redes cabeadas, e ambas tornam-se nós vulneráveis à um ataque. Neste caso, serviços adicionais de segurança são necessários para evitar que um violador possa acessar a rede cabeada, mesmo se este for capaz de acessar a rede sem fio. Não será suficiente proteger a conexão à Internet utilizando firewalls se a rede tiver um ponto de acesso sem fio como porta dos fundos (backdoor). São necessários serviços especiais de segurança nos pontos de acesso.

Estas redes podem também ser conectadas a outras redes sem fio formando uma rede maior. Este tipo de rede é chamada multi-passo ad hoc porque os dispositivos atuam como roteadores e enviam mensagens aos destinatários. O maior problema de segurança nesta rede é relacionado ao roteamento.

3.8 Roteamento

Para redes ad hoc, o roteamento de pacotes entre nós é um desafio, uma vez que os nós podem mover-se aleatoriamente na rede e, um caminho válido em um momento pode, simplesmente, não existir num momento seguinte. Além disso, as propriedades estocásticas de canais sem fio interferem na qualidade do caminho. O ambiente operacional pode causar problemas adicionais, como o fechamento de uma porta pode romper um caminho da rede.

Os protocolos de roteamento tradicionais são pró-ativos; porque eles mantêm as rotas de todos os nós da rede, incluindo rotas ligadas aos nós que não estejam enviando ou recebendo pacotes. Eles são reativos a qualquer modificação na topologia da rede se o tráfico não for corrompido, e requerem o controle de mensagens para manter as rotas válidas.

Por outro lado, as redes ad hoc envolvem o estabelecimento de rotas reativas, o que faz com que as rotas entre nós sejam definidas somente quando necessário. Isto evita a constante atualização das informações sobre cada rota da rede, e permite se dedicar mais atenção às rotas realmente em uso.

Deste modo, para encorajar a disponibilidade, os protocolos de roteamento devem ser resistentes a modificações na topologia da rede e a ataques. Os protocolos de roteamento sugeridos para redes ad hoc suportam a troca dinâmica de topologia; no entanto, nenhum destes protocolos possui mecanismos de segurança à ataques.

Em um ambiente de comunicação sem fio, o tráfico que viaja através da rede ad hoc é vulnerável a ameaças na segurança. Uma rede ad hoc está sujeita a outras ameaças na estrutura básica da rede.

Existem, no entanto, técnicas para assegurar que as transações de aplicações, em protocolos de rede tradicionais, possam ser aplicadas em redes ad hoc.

[ZHOU99] mostra alguns aspectos importantes na segurança de redes ad hoc. Em primeiro lugar, o uso de conexões sem fio é suscetível a ataques na conexão. Podem acontecer ataques passivos, tais como um espião passivo em um dispositivo ilegal ativo que coleta e informa ao adversário uma informação secreta, causando uma violação da confidencialidade. Também, ataques ativos permitem a exclusão de mensagens, inclusão de erros em mensagens, modificação de mensagens e a transformação de um nó não autorizado em um elemento de rede válido e

autorizado, além da violação à disponibilidade, integridade, autenticação e ao não repúdio.

Além disso, nós em trânsito com uma proteção fraca têm uma maior probabilidade de serem comprometidos por elementos externos. A rede ad hoc é, inclusive, dinâmica devido à constante mudança em sua de topologia e ao número variável de nós. Isto pede soluções de segurança escaláveis e adaptativas.

Os tipos de ataques em roteamento podem ser classificados de acordo com a seguinte tabela:

Tabela 1: Tipos de Ataque em roteamento ad hoc

Ataques Passivos	Captura de mensagens de roteamento e envio a terceiro não autorizado.
Ataques Ativos	Fabricação ou modificação de informação de roteamento
	Loops de roteamento.
	Congestionamento da rede.
	União ou fragmentação da rede
	Interrupção total da rede

Outro aspecto na segurança do roteamento ad hoc é a relação entre os serviços de segurança em redes e ataques potenciais às funções de roteamento nas redes ad hoc. A Tabela 2 mostra tal interação:

Tabela 2: Relação entre serviços de segurança e ataques em roteamento ad hoc

Disponibilidade	Camadas Física e de Controle de Acesso ao Meio: interferência da comunicação nos canais físicos (jamming) Camada de Rede: Corrupção do protocolo de roteamento e a desconexão da rede. Camadas Superiores: Derrubar serviços de alto nível, como o gerenciamento de chaves, essencial para a manutenção da segurança.
Confidencialidade	Perda da confidencialidade das informações de roteamento .
Integridade	Informações de roteamento adulteradas podem ser detectadas e descartadas.
Autenticidade	Rotas de dispositivos autenticados podem ser atualizadas.
Não Repúdio	Identificação e isolamento de nós adulterados. Se um nó A recebe de um nó B uma mensagem errada, o não repúdio permite que A acuse B de ser um nó adulterado.

Contudo, os mecanismos de segurança, como protocolos de autenticação, assinatura digital e criptografia ajudam a manter a confidencialidade, integridade, autenticidade e não repúdio em redes ad hoc, mas isto não é suficiente. Por este

motivo existe, no projeto de uma rede ad hoc, a vantagem da redundância da topologia (múltiplas rotas entre nós) que favorece a disponibilidade. Uma outra solução para assegurar que os nós sejam confiáveis é a distribuição de confiança, onde um nó só é confiável se outros nós o confirmarem (detalhes na sessão sobre distribuição de confiança em 3.13.2.

3.9 Mecanismos de segurança para redes Ad-Hoc

3.9.1 Segurança no Meio Físico

O meio físico de transmissão utilizado pela tecnologia Bluetooth e por quase todos os protocolos de comunicação IEEE 802.11 é o espalhamento espectral.

O espalhamento espectral (SS, Spread Spectrum) é um mecanismo desenvolvido durante a Segunda Guerra Mundial para estabelecer um canal de comunicação seguro e confiável no campo de batalha. Existem diversas técnicas utilizadas para implementar um método SS de comunicação, que são: seqüência direta (Direct Sequence) (DS), salto de freqüência (Frequency Hopping) (FH) e salto no tempo (Time Hopping) (TH), além de algumas técnicas híbridas formadas a partir das técnicas mencionadas acima.

Os protocolos de comunicação Bluetooth e IEEE 802.11 utilizam especificamente DS-SS e FH-SS. Somente estas técnicas estão descritas a seguir.

3.9.2 Espalhamento Espectral do tipo Direct Sequence - DS-SS

DS-SS foi o primeiro protocolo de comunicação por espalhamento espectral a ser desenvolvido e funciona espalhando um sinal de comunicação de banda estreita em um sinal de comunicação de banda larga, através da utilização de um código independente do conteúdo da informação. O receptor deve usar o mesmo código com sincronismo perfeito para extrair a informação desejada [JESZ91] [JESZ92]. Uma banda de comunicação é uma faixa delimitada do espectro de freqüência utilizado na comunicação entre dois ou mais pontos.

DS-SS espalha o sinal de banda estreita transmitido com a multiplicação do sinal original por uma seqüência pseudo aleatória, produzida por um gerador de código pseudo aleatório.

A privacidade e confiabilidade da comunicação é garantida através do uso de sistemas SS, pois para receber a mensagem transmitida é necessário ter conhecimento prévio da seqüência pseudo aleatória utilizada. Além disso é possível compartilhar o mesmo espectro de freqüência com muitas outras comunicações simultâneas.

$$s(t) = A \cdot m(t) \cdot \cos(\omega_0 \cdot t + \theta)$$

Equação1 – Sinal digital antes da transmissão

$$s(t) = A \cdot m(t) \cdot d(t) \cdot \cos(\omega_0 \cdot t + \theta)$$

Equação 2 - Sinal digital após multiplicação do código.

Para a equação acima devemos considerar:

$m_i(t) = \pm 1$ para intervalo $k \cdot T_c \leq t < (k+1) \cdot T_c$, com $k = 0;1;2....$

$d_i(t) = \pm 1$ para intervalo $j \cdot T \leq t < (j+1) \cdot T$, com $j = 0;1;2....$

sendo T_c o período da ocorrência de bit de dados e T o período da ocorrência de bit de dados, onde $T >> T_c$.

É difícil obter confidencialidade com mensagens analógicas [DILL89]. As mensagens analógicas de amplitude modulada (AM) podem ser facilmente recuperadas com um simples detetor de envelope. As mensagens analógicas de freqüência modulada (FM) também podem ser facilmente recuperadas, utilizando detetores de freqüência (método direto) ou com circuitos phase lock loop (PLL) e demoduladores FM com realimentação (FMFB) [CABR99].

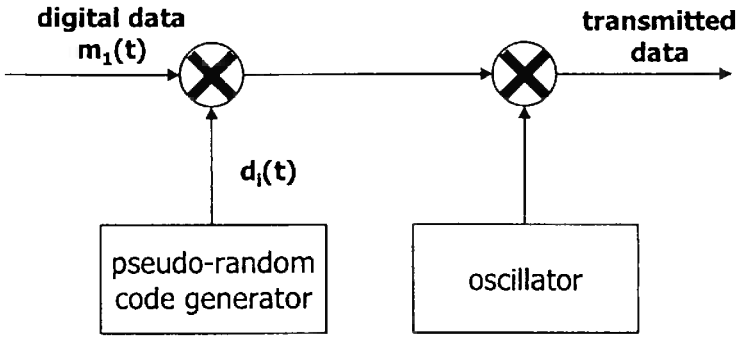


Figura 9: Circuito de Transmissão [TORR85]

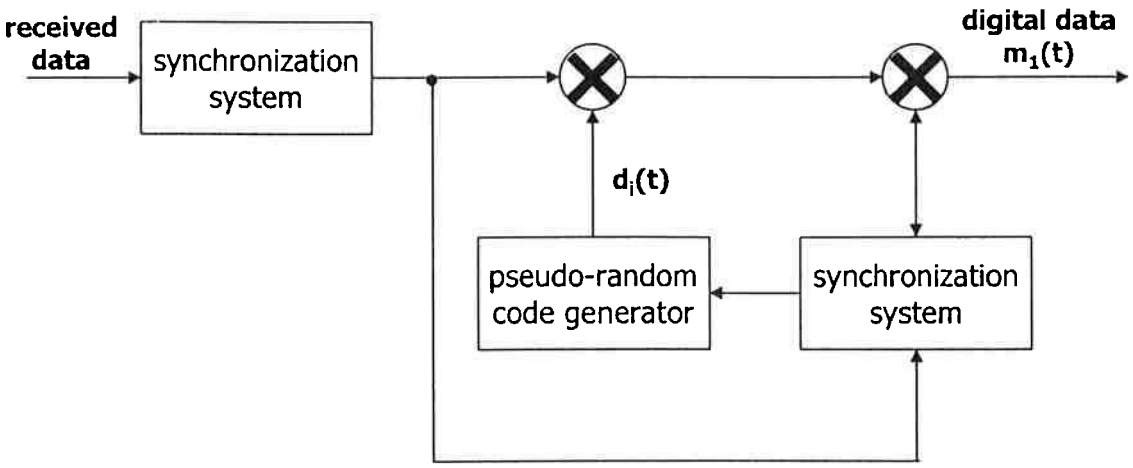


Figura 10: Circuito de Recepção [TORR85]

É difícil detectar o DS-SS quando se utiliza uma análise espectral simples pois a densidade espetral é baixa em comparação ao ruído térmico. A densidade espetral também muda vagarosamente dentro da largura da banda, tornando a identificação da comunicação muito difícil. Estes fatores aumentam a confidencialidade da comunicação DS-SS.

DS-SS pode também evitar interferência, intencional ou não, usando a multiplicação de código pseudo aleatória durante o processo de recepção. Isto acontece porque todos os sinais recebidos são multiplicados pelo código e um sinal eventual de jamming seria espalhado através de todo o espetro. Outras comunicações DS-SS seriam também rejeitadas, porque os códigos pseudo aleatórios utilizados na sua multiplicação são diferentes entre si.

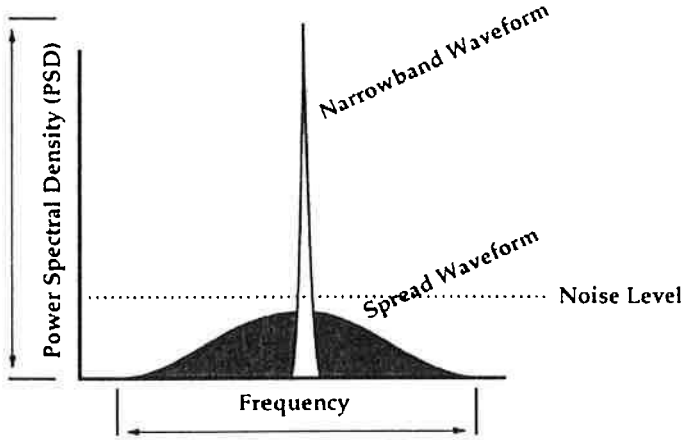


Figura 11: Densidade espectral da potência de um sinal espalhado (DS-BPSK) sob efeito de interferência

3.9.3 Frequency Hopping Spread Spectrum – FH-SS

FH-SS espalha a transmissão em uma largura de banda determinada alternando periodicamente entre as freqüências de uma dada largura de banda, seguindo uma seqüência determinada definida por uma seqüência pseudo aleatória. O receptor deve ser sincronizado com o transmissor para tornar a recepção possível [JESZ91].

O FH-SS consome menos energia do que o DS-SS, e é recomendado para aparelhos portáteis (móveis) alimentados por pilhas.

É importante saber que há dois tipos de comunicação FH-SS. A FH-SS Rápida (FFH-SS) e a FH-SS (SFH-SS) Lenta. A diferença entre os dois modos é a velocidade com que a freqüência muda durante a comunicação.

Resumindo, em uma comunicação FFH-SS o tempo de transmissão de um símbolo é maior que o tempo entre dois saltos de freqüência, o que significa que um símbolo é parcialmente transmitido em uma única freqüência. Na comunicação SFH-SS ocorre o oposto, isto é, um ou mais símbolos são transmitidos um uma única freqüência.

Assim como a DS-SS, a FH-SS oferece privacidade de comunicação porque é extremamente difícil rastrear um sinal FH-SS sem o conhecimento prévio da seqüência pseudo aleatória utilizada em uma comunicação [DILL89].

A FH-SS pode também evitar interferência, tanto quanto a DS-SS, intencional ou não, porque pode evitar freqüências comprometidas.

3.10 Acesso Não Autorizado à Rede

3.10.1 802.11

A segurança de conexão de dados IEEE 802.11 é composta pela autenticação do usuário e pela privacidade da comunicação, e é baseada em um algoritmo conhecido como Wired Equivalent Privacy (WEP).

3.10.1.1 Autenticação

A autenticação IEEE 802.11 é feita para evitar problemas de controle de acesso à rede sem fio, e pode ser feita de duas formas distintas. IEEE 802.11 [802.11] define os modos de autenticação Open System e Shared Key.

A autenticação é feita entre o Ponto de Acesso sem fio (AP, Access Point) e a estação que quer se comunicar com a rede. É importante notar que este é um método de autenticação de mão única. A autenticação mútua é usada para comunicações diretas entre duas estações, sem a presença de um AP.

O método de autenticação Open System é o mais simples, na verdade sendo uma autenticação nula. Este método é o padrão IEEE 802.11. Uma autenticação Open System unidirecional tem somente duas etapas. Na primeira, a estação que quer se comunicar envia uma solicitação com seu ID. A segunda etapa é a resposta, baseada no ID enviado.

A autenticação Shared Key requer o conhecimento mútuo de uma chave secreta entre os participantes do processo de autenticação. Uma autenticação unidirecional é feita em quatro etapas através da utilização do algoritmo WEP (Figura 122)

A primeira etapa é a solicitação de autenticação enviada pela estação que quer se comunicar. Na segunda, o AP ou a estação que recebe o pedido envia uma mensagem-desafio para a primeira estação. Essas duas mensagens mencionadas acima são enviadas em formato texto limpo, ou seja, sem criptografia.

O desafio então é criptografado na terceira etapa, com a chave secreta (e compartilhada) usando o algoritmo WEP, e enviado de volta ao AP (ou estação) que gerou o desafio. Na Quarta e última etapa a mensagem é enviada para a estação solicitando uma resposta positiva ou negativa do processo de autenticação. Esta última mensagem é enviada em formato de texto limpo, sem criptografia, para evitar a criptoanálise.

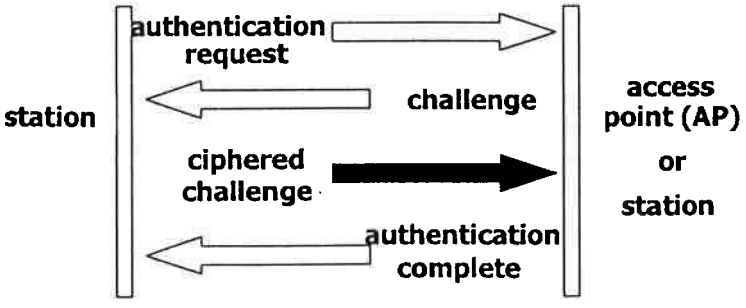


Figura 12: Método de autenticação Shared Key

3.10.1.2 *Wired Equivalent Privacy (WEP)*

A confidencialidade é conseguida com o algoritmo WEP [802.11]. O WEP é utilizado como uma proteção para usuários autorizados contra ataques de captura de informações. Este serviço visa fornecer aos usuários de rede sem fio um nível de segurança equivalente ao da segurança de rede com fio. O uso do WEP é opcional em uma rede IEEE 802.11.

O WEP trabalha no nível de enlace, cifrando os dados (note que o cabeçalho IP e de níveis superiores estão cifrados). Isto significa que a criptografia ocorre somente entre a estação e o AP, sendo decifrado neste ponto para permitir que a mensagem viaje em um meio físico com fio, considerado historicamente seguro (!).

WEP utiliza um gerador de números pseudo-aleatório baseado no algoritmo RC4 com uma semente de 64bits, dos quais 40bits pertencem à chave secreta e os 24bits restantes ao Initialization Vector (IV). Os diagramas de codificação e decodificação usando o WEP estão representados na Figura 13 e na Figura 14, respectivamente. Repare que o IV é transmitido sem codificação.

PRNG - Pseudo Random Number Generator

|| - concatenation

⊕ - bitwise XOR

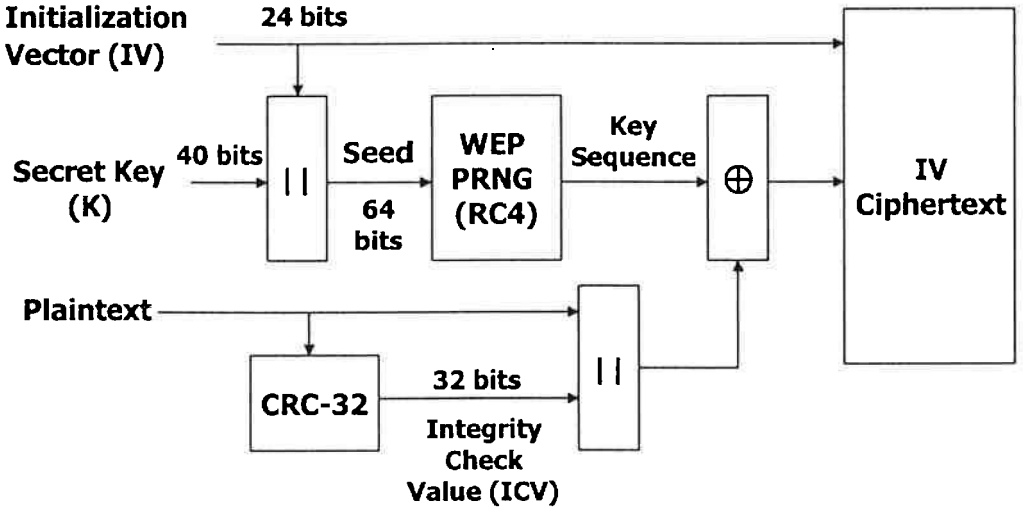


Figura 13: Cifragem WEP

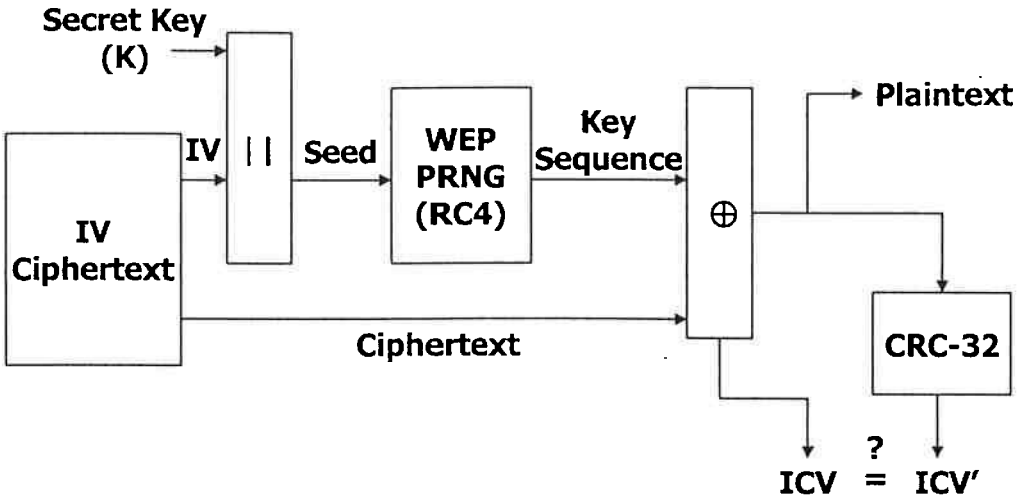


Figura 14: Decifração WEP

3.10.1.3 Considerações adicionais sobre Segurança IEEE 802.11

O esquema de segurança IEEE 802.11 possui algumas falhas, como a não obrigatoriedade de autenticação mútua quando uma estação quiser se comunicar com um AP. Isto permite que um AP intruso aja como um AP autorizado, e possivelmente obtenha informações sigilosas.

WEP é suscetível a ataques repetidos (replay) [BALL01] porque não possui nenhum controle de seqüência de quadros, nem uma associação de tempo com os dispositivos conectados.

Outra questão importante é a falta de gerenciamento de chaves e mecanismos de distribuição da mesma na especificação. Além disso, a especificação define somente uma chave compartilhada para todos os usuários. Isto pode causar sérios problemas pois se um usuário perder a chave ou se ela for decifrada por alguém, será necessário mudar todas as chaves de todos os usuários.

O processo de autenticação é vulnerável a ataques do tipo man-in–the-middle porque a mensagem-desafio viaja limpa e é então codificada, e pode estar sujeita à criptoanálise para obter a senha ou mesmo a chave secreta.

E finalmente, o fato dos 24 bits do IV serem transmitidos em texto limpo (sem codificação) é um ponto fraco do WEP e limita a sua resistência a ataques de força bruta. Além disso, o RC4 de 40 bits é considerado, hoje em dia, como um algoritmo fraco de criptografia.

3.10.2 Bluetooth

A especificação Bluetooth tem por objetivo garantir a segurança nos níveis físico e de enlace. No nível físico utiliza a técnica de espalhamento espectral do tipo salto em freqüência (FHSS, Frequency Hop Spread Spectrum) e devido a baixa potência de transmissão oferece proteção contra intercepções e interrupções, enquanto que no nível de conexão oferece serviços de autenticação e criptografia.

Cada tipo de rede e serviço oferecido exige níveis diferentes de segurança em relação aos dados, aplicações e dispositivos. Para que a oferta de serviços de

segurança em nível de enlace seja flexível, a especificação Bluetooth define três modos de segurança: modos 1, 2 e 3. Estes modos usam basicamente três tipos de serviços: Pairing, autenticação e criptografia. O processo de pairing oferece uma maneira segura de mudar a chave de enlace. Durante o processo três tipos de chaves são utilizados: chave de inicialização, chave de enlace e chave de criptografia.

3.10.2.1 Modos de Segurança

Há três modos de segurança definidos na especificação Bluetooth [BLUE01B]:

- Modo de Segurança 1 - Inseguro: O modo 1 é um modo não seguro onde nenhum procedimento de segurança é executado;
- Modo de Segurança 2 – Serviço seguro: O modo 2 oferece segurança definida pelo serviço, permitindo flexibilidade quando vários aplicativos estiverem rodando. Neste modo um canal lógico é estabelecido inicialmente e os procedimentos de segurança são exigidos depois, dependendo dos requisitos do serviço ou do canal. Os serviços de segurança fornecidos pelo Bluetooth são autenticação, autorização e criptografia. A autenticação é obrigatória para as autorizações de acesso. A criptografia é opcional, dependendo dos serviços;
- Modo de Segurança 3 – Enlace Seguro: Neste modo nenhum canal lógico é estabelecido antes que os procedimentos de segurança sejam concluídos. O dispositivo Bluetooth trabalhando neste modo pode rejeitar um dispositivo que não foi previamente registrado no processo de pairing, por exemplo. A autenticação é obrigatória e a criptografia é opcional.

3.10.2.2 Serviços de Segurança

Bluetooth oferece serviços de autenticação e de criptografia em nível de enlace. Por utilizar um método de criptografia de chave simétrica (chave compartilhada), esta chave deve ser definida inicialmente ou deve ser estabelecido um meio seguro para a mudança de chave. O processo de emparelhamento ("pairing") é responsável por inicializar um processo de troca de informações entre os dispositivos para estabelecer uma chave de inicialização (chamada K_{init}), que é usada para autenticar o dispositivo e no processo para criar uma chave de enlace (chamada K). A chave de enlace é usada no processo de autenticação e estabelecimento de um canal seguro, para gerar a chave de criptografia [BLUE01A].

Bluetooth trabalha com quatro parâmetros de segurança: o endereço do dispositivo (BD_ADDR), duas chaves secretas e um número aleatório. O BD_ADDR é um endereço de 48-bit, IEEE MAC único. Os quatro parâmetros são combinados para compor as chaves utilizadas nos procedimentos de segurança.

Parâmetros de Segurança	Extensão
BD_ADDR	48 bits
Chave pessoal do usuário – autenticação	128 bits
Chave pessoal do usuário – encriptação	8 to 128 bits
Número aleatório	128 bits

Tabela 3: Entities usadas na segurança Bluetooth

Além dos parâmetros de segurança acima, o dispositivo Bluetooth possui um Número de Identificação Pessoal (PIN, Personal Identification Number) que pode ser utilizado nos serviços de segurança.

Quatro algoritmos são utilizados nos procedimentos de segurança, chamados de algoritmos E_0, E_1, E_2 and E_3. O algoritmo E_2 tem dois modos de operação, chamados E_{21} e E_{22}, dependendo da chave a ser criada. Os algoritmos E_{21} e E_{22} são usados para criar a chave de enlace, que será usada para autenticar os dispositivos. O algoritmo E_1 é usado durante o processo de autenticação e parte de seu resultado é usado para criar a chave de criptografia. Finalmente, o algoritmo E_3 é usado par gerar uma chave de criptografia de sessão (K_C), que é utilizado pelo algoritmo E_0 para criptografar os dados. Os procedimentos de segurança e os algoritmos utilizados são detalhados abaixo. Esses algoritmos são em parte baseados no algoritmo de criptografia SAFER+ (Secure And Fast Encryption Routine) [BLUE01A].

3.10.2.2.1 Pairing – Procedimento de Inicialização

Este procedimento inicia-se quando dois dispositivos nunca se comunicaram um com o outro e assim não compartilham a mesma chave de enlace. Após a criação da chave de inicialização, inicia-se um processo de autenticação com o objetivo de identificação. Posteriormente, uma nova chave de enlace é criada por um processo de mudança de chave, como demonstrado na Figura 15: .

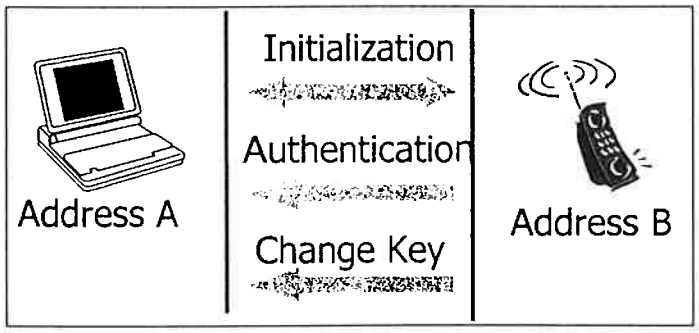


Figura 15: Procedimento Paring

A chave de inicialização, K_{Init}, é criada a partir do endereço do dispositivo, um número PIN, um número aleatório (RAND) e o comprimento do número PIN (L), como mostra a Figura 16. O número PIN pode ter até 128 bits (0 a 16 octetos). A chave de enlace K_{Init} tem 128 bits [BLUE01A].

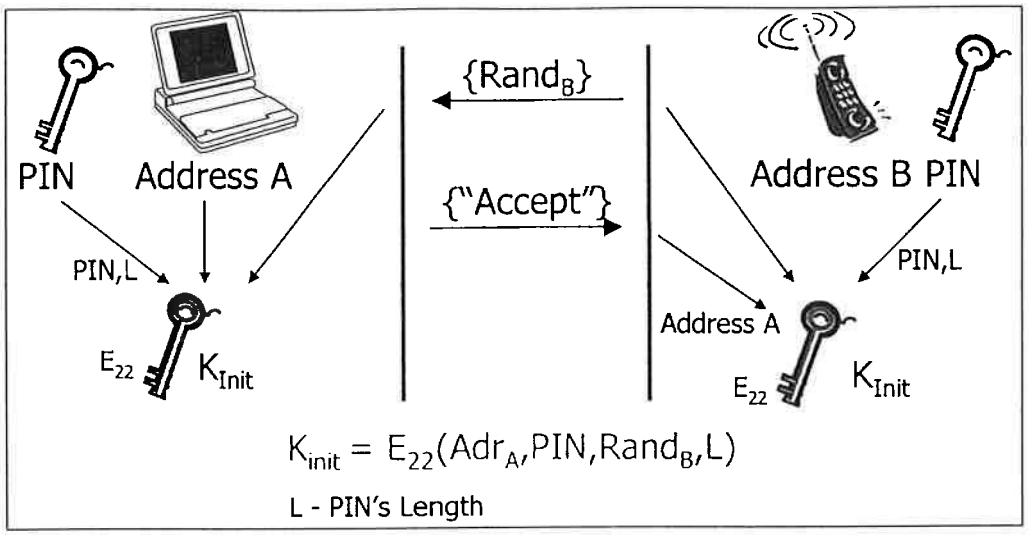


Figura 16: Procedimento de Criação da Chave de Inicialização

Os dispositivos podem atuar em dois modos, com ou sem pairing:

- Modo sem pairing: Recusa o pedido de pairing.
- Modo com pairing: Quando um dispositivo enviar a solicitação de pairing ao outro, pode ocorrer:
  - Se o dispositivo tem um PIN variável, aceita o pairing.
  - Se o dispositivo tem um PIN fixo, retorna com uma solicitação de pairing.
  - Se ambos tem um PIN fixo a solicitação é recusada.

3.10.2.2.2 Autenticação

O procedimento de pairing é executado somente uma vez para fornecer uma conexão segura para a troca da chave de enlace. Após a criação da chave de enlace, a chave K_{init} pode ser esquecida. Sempre que os dois dispositivos se comunicarem eles irão utilizar a chave de enlace secreta negociada. A chave de enlace é utilizada para autenticação de dispositivo através do procedimento de desafio-resposta. Quando a autenticação falha, o tempo de espera do dispositivo para novas tentativas aumenta exponencialmente, para dificultar um ataque de força bruta [BLUE01A].

A unidade verificadora envia um número aleatório para a unidade a ser autenticada ($RAND_A$); o dispositivo receptor aplica um algoritmo de autenticação chamado E1,que utiliza como parâmetro o número aleatório recebido, seu endereço e a chave de enlace. O resultado do algoritmo, SRES (Signed RESponse), é enviado para a unidade de verificação, que executa o mesmo algoritmo, usando os mesmos parâmetros. Se os resultados forem iguais, a unidade B é autenticada. O processo de autenticação é mostrado na Figura 17.

O algoritmo E_1 usado para autenticação resulta em duas saídas chamadas SRES e ACO (Authenticated Ciphering Offset). O SRES de 32 bits é usado durante o processo de autenticação e o ACO de 96 bits é usado durante o processo de geração da chave de criptografia.

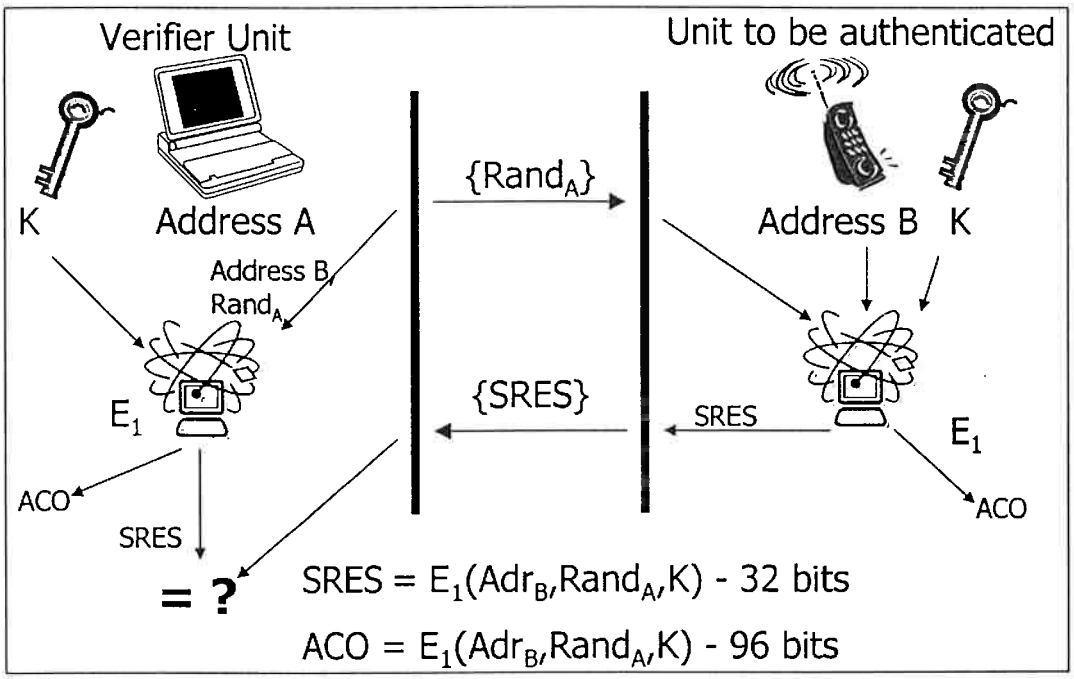


Figura 17: **Procedimento de Autenticação.**

3.10.2.2.3 Mudança da Chave de enlace

Uma nova chave de enlace pode ser gerada a qualquer momento. Em particular, quando uma chave de inicialização é gerada para a chave de enlace inicial, ela deve ser modificada [BLUE01A].

Além da chave de inicialização, há dois outros tipos de chave de enlace, a chave da unidade e a chave de combinação. A chave da unidade é usada quando um ou ambos dispositivos não permitem a inserção manual de um código PIN; quando ambos permitem, a chave de combinação é gerada. A chave de inicialização é usada primeiro como uma chave de enlace. Se um dispositivo utiliza uma chave de unidade, então esta é a única chave que precisa ser armazenada. Se um dispositivo utiliza uma chave de combinação então deve armazenar uma chave de enlace para cada dispositivo que se comunica com ele.

A Figura 18 mostra o processo de mudança de chave usando uma chave de combinação. Dois números aleatórios são trocados entre os dispositivos que querem modificar a chave de enlace. Somente A e B conhecem os números aleatórios porque eles estão criptografados com a chave de enlace atual e ambos pode criar as chaves K_A e K_B. A chave K_A é criada usando o endereço de A e o número aleatório criado por A; a chave K_B é criada de modo semelhante. A chave de combinação K_{AB}

é criada pela adição simples em modulo-2 bit-a-bit (e.g. XOR) das duas chaves criadas.

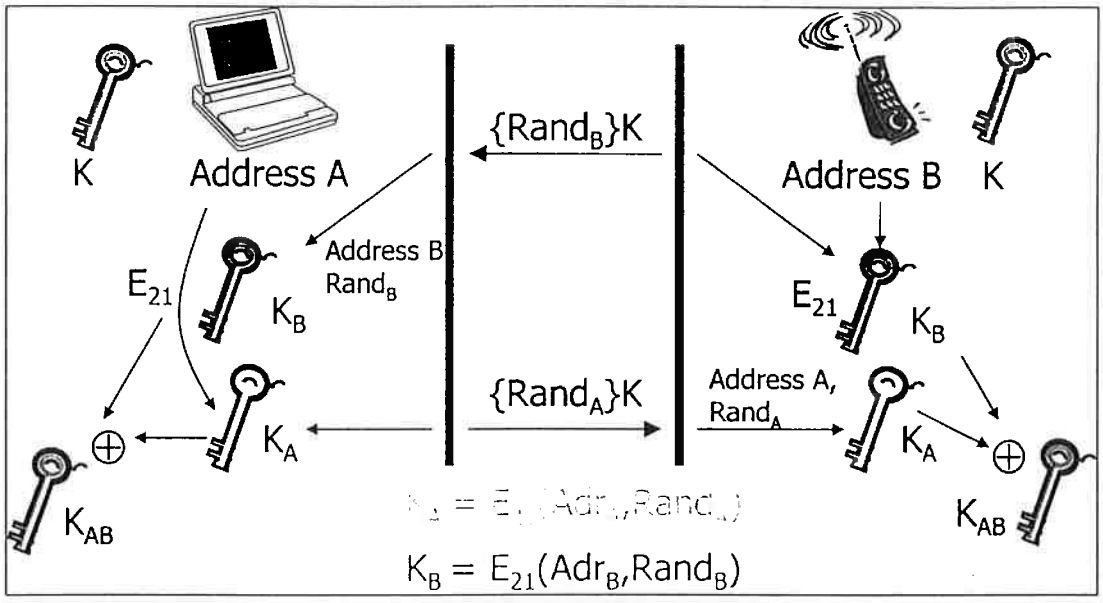


Figura 18: Procedimento de Mudança de Chave

A chave de enlace pode ter valores diferentes a cada momento, e portanto o termo chave de enlace atual é usado para definir a chave de enlace que está sendo usada naquele momento. Durante o processo de pairing a chave K_{init} é utilizada como chave de enlace até que o processo de mudança de chave esteja finalizado. Neste momento, a chave de combinação torna-se a nova chave de enlace atual, K_{AB}. Quando os dispositivos não permitem a geração de uma chave de combinação, como aqueles que possuem um PIN fixo, então a chave de enlace atual pode ser a chave da unidade, K_A. Quando o master desejar fazer uma transmissão para os slaves, ele deve usar uma outra chave como chave de enlace; que é chamada de chave master, K_{Master}. Um procedimento de troca da chave de enlace para a chave master é temporariamente realizado, voltando para a chave de enlace no final do processo.

3.10.2.2.4 Criptografia

O uso de criptografia em nível de enlace [BLUE01A] tem por objetivo manter uma comunicação secreta. Existem diversos modos de criptografia que podem ser utilizados por um dispositivo Bluetooth usando uma chave temporária (chave de unidade ou chave de combinação) ou chave *master* para geração de uma chave criptográfica. Quando uma chave temporária é utilizada, apenas o tráfego individual pode ser criptografado. Para se criptografar o tráfego broadcast é necessária a utilização de uma chave master e caso a chave master seja a chave de enlace corrente, o tráfego individual também utiliza essa chave para a geração de chave de criptografia. O procedimento de criptografia requer três fases, primeiro é necessário se negociar o modo de criptografia e o comprimento da chave a ser utilizada; o

algoritmo suporta diferentes comprimentos de chave. Posteriormente, a chave de criptografia é gerada e finalmente o algoritmo de criptografia é aplicado. O processo é mostrado na Figura 19.

A chave de criptografia K_C de 96 bits é gerada, para cada conexão, usando a chave de enlace corrente, um número aleatório e uma variável COF (Ciphering Offset Number), que é igual ao valor de ACO gerado pelo algoritmo de autenticação, quando uma chave master não é utilizada ou for igual a $BD\_ADDR_{MASTER} \cup BD\_ADDR_{MASTER}$[2] se uma chave master for utilizada. A utilização de um comprimento menor de chave é possível sem que haja uma redução na segurança porque a chave de criptografia é alterada a cada conexão.

Bluetooth faz uso de um algoritmo de criptografia do tipo em cadeia ("stream"), que é baseado no LFST (Linear Feedback Shift Register), que processa os parâmetros de entrada em uma máquina de estado finito simples, chamada Summation Combiner, onde as saídas do algoritmo LFST são combinadas em uma cadeia de bits C. Esta cadeia de bits é então somada bit-a-bit em módulo-2 ao dado, gerando um fluxo criptografado.

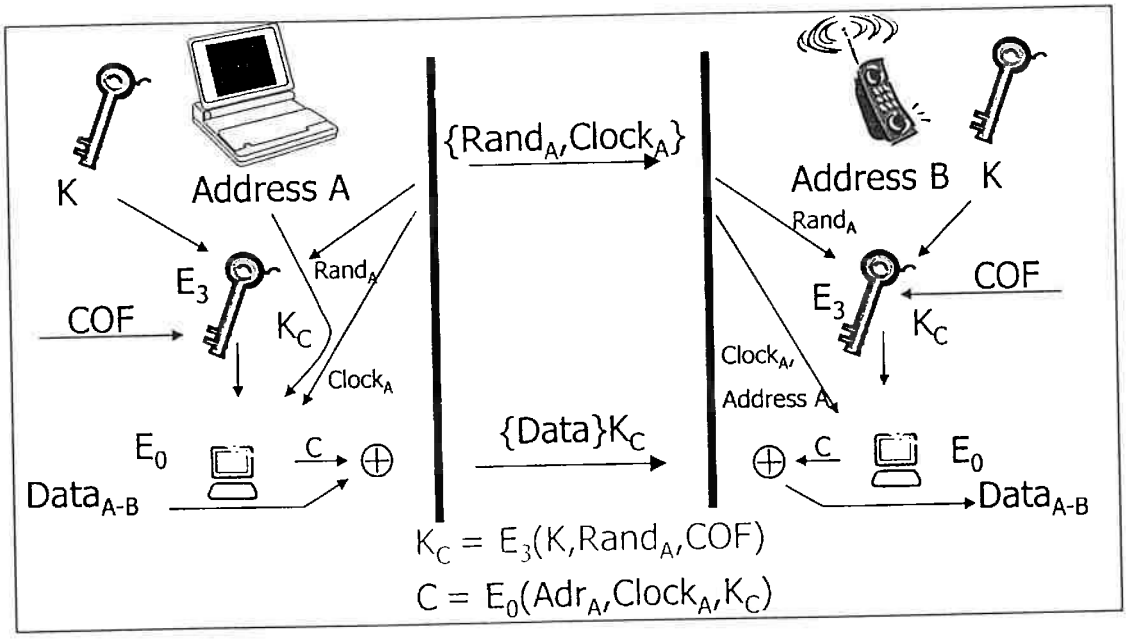


Figura 19: Procedimento de geração de chave de criptografia e aplicação de algoritmo.

3.10.2.3 Considerações adicionais de Segurança Bluetooth

Toda a segurança Bluetooth é baseada em uma chave de enlace que é usada para autenticar o dispositivo e gerar uma chave criptografada. A chave de enlace é criada baseada em uma chave de inicialização, cuja força está exclusivamente no código secreto PIN. Como o código PIN necessita ser inserido duas vezes a cada vez que dois dispositivos são conectados pela primeira vez e é usualmente inserido pelo usuário, o PIN tende a ser curto e algumas vezes coincidente. Isto pode facilmente comprometer a segurança..

[2] $BD\_ADDR \cup BD\_ADDR$: concatenação de bits.

A especificação sugere que o código PIN deva ser fornecido pelo aplicativo com um número maior de bits. O código PIN pode ser exportado para outros dispositivos de acordo com o protocolo Diffie-Hellman, por exemplo.

Bluetooth utiliza um processo de desafio-resposta para autenticar dispositivos. Este mecanismo é defectivo quando uma chave de unidade é utilizada. Quando um dispositivo A possui um PIN fixo, ele tem que usar esse PIN para gerar uma chave de enlace para uma comunicação segura com outros dispositivos. Como o PIN no dispositivo A é o mesmo para comunicação com outros dispositivos, não é difícil para o dispositivo B se autenticar ao dispositivo A como sendo o dispositivo C.

Um outro problema é o Endereço de Dispositivo Bluetooth, que é único para todo e qualquer dispositivo Bluetooth. Este número é utilizado a cada conexão, e subseqüentemente um dispositivo pode usar esta informação para rastrear e monitorar o comportamento do proprietário de um dispositivo. Logs podem ser registrados para cada transação e a privacidade pode ser violada.

Em [HERM99] são apresentadas algumas vulnerabilidades no esquema de criptografia Bluetooth. Este documento mostra que o algoritmo de criptografia do tipo stream do Bluetooth com chave de 128 bits pode ser quebrado em $O(2^{64})$.

Em [TRÄS00], são tratadas questões relativas à autenticação de usuário e autorização para utilização de serviços individuais . A especificação Bluetooth inclui dispositivos de segurança em nível de enlace, mas uma solução de segurança fim-a-fim não é comentada. A autenticação do dispositivo também é especificada, mas não a autenticação do usuário. O controle de autorização é efetuado mas as funções são válidas para todos os serviços e o controle de acesso individual aos serviços não é mencionado. Baseado em tudo o que foi mencionado, deve-se considerar a existência de uma solução de segurança em mais alto nível.

Finalmente, no processo de autenticação, desafio-resposta, o número aleatório é passado sem criptografia e retorna na forma criptografada, o que permite o ataque do tipo man-in-the-middle.

Algumas modificações foram implementadas para aperfeiçoar a segurança Bluetooth, mas continuam limitadas ao nível de enlace. Soluções de segurança num nível mais elevado precisam ser especificadas de modo que o aplicativo de segurança possa usar a tecnologia Bluetooth com segurança.

3.11 Acesso Não Autorizado a Informações

Neste capítulo foram mostrados alguns mecanismos utilizados pelo padrão 802.11 e pela tecnologia Bluetooth para fornecer serviços de segurança. Estes mecanismos se aplicam aos níveis físico e de enlace, o que limita o seu raio de ação. Estes mecanismos tentam controlar quais dispositivos são reconhecidos e podem fazer parte da rede. O controle de acesso trabalha num nível mais alto de protocolo.

A segurança de informação em redes sem fio não difere daquelas da rede por fio mas alguns mecanismos precisam ser acrescentados para que se garanta, de fato essa segurança. Em uma rede por fios, diversos níveis de segurança são introduzidos para proteger as redes locais de ataques. Geralmente o primeiro nível de segurança é um *firewall*, que procura delimitar o que pode entrar numa rede local.

Numa rede infra-estruturada sem fio, um controle similar pode ser adicionado em um ponto de acesso. No entanto, em redes *ad hoc*, não há um equipamento que regule o que chega através da rede; conseqüentemente cada dispositivo é responsável pela segurança de toda rede.

Sem a presença de um *firewall* comum, um tipo de *firewall* necessita ser inserido em cada dispositivo para sua própria proteção. Cada dispositivo necessita de uma lista de controle de acesso de todos os serviços, dispositivos e usuários com os quais ele possa interagir. Para um controle de acesso bem sucedido, é necessário que se faça um processo eficiente de autenticação de dispositivos, usuários e serviços. O mecanismo de certificação e de assinaturas digitais precisa ser utilizado para permitir algum controle na interação através da rede.

Do mesmo modo que clientes não autorizados podem tentar fazer uso de serviços, serviços fraudulentos podem ser oferecidos aos clientes. Numa rede baseada em serviços, a segurança dos clientes também precisa ser assegurada. Algumas vezes a integridade e as assinaturas dos serviços precisa ser verificada para que se evitem ataques de *worm*, vírus ou o oferecimento fraudulento de serviços.

Um outro aspecto que torna as questões de integridade e de assinaturas mais desafiadoras em ambientes de rede *ad hoc* é a mobilidade intrinsecamente associada à maioria dos pontos de conexão de tais redes. A natureza temporária do estado dos nós precisa ser lidada com grande cuidado a fim de garantir segurança suficiente sem que haja perda na conveniência da mobilidade.

Uma rede *ad hoc* precisa ser flexível para manter o oferecimento de serviços simples, como exportar "Cartões de Visita Virtuais" e "obter dados acerca de vôos em aeroporto", para os quais não há necessidade de controles de segurança, mas também deve ter acesso a serviços controlados. O principal desafio é fazer uso de um serviço de segurança com a mínima intervenção do usuário e com mecanismos de segurança simples e eficientes, evitando assim problemas de capacidade e de performance.

3.12 Distribuição de Confiança

Quando uma rede *ad hoc* é voluntariamente criada entre entidades num mesmo local, não há garantias de que um nó distribua a sua chave pública de modo confiável ou de que se apresente com certificados digitais confiáveis para todos os seus companheiro ou pontos de acesso. Além disso, é possível delegar confiança a outros nós, estabelecendo uma cadeia de confiança podendo estender esta relação a outros nós da rede.

Em [FRJO 00], a confiança pode ser distribuída entre um conjunto de nós, sem se considerar ataques de recusa de serviço nos níveis físicos e de enlace. Este método é baseado numa aproximação da chave pública. Primeiro, assume-se que a há conectividade entre todos os pontos de conexão da rede e que um protocolo de roteamento reativo possa ser mantido. Este processo é exibido da Figura 20 à Figura 23.

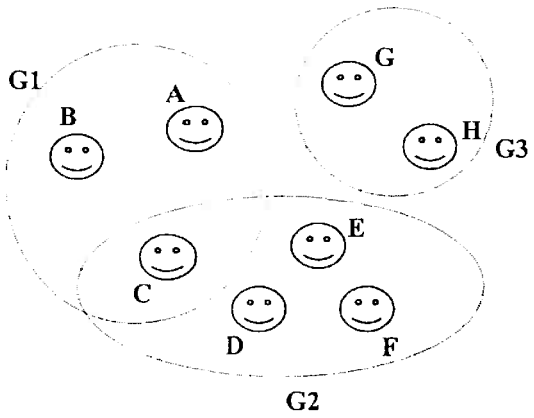


Figura 20: Distribuição de Confiabilidade – 1ª Fase

Esta é uma rede *ad hoc* separada em três grupos de confiança: G1, G2 e G3. Nesta fase, uma troca segura de dados de dados de segurança não pode ocorrer entre os nós porque o único nó confiável para G1 e G2 é o nó C.

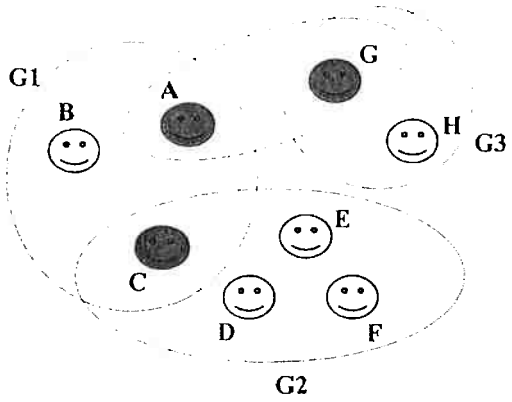


Figura 21: Distribuição de Confiabilidade – 2ª Fase

O nó C envia para A as chaves Públicas assinadas (certificadas) dos nós D, E e F dizendo que D, E e F são confiáveis. Adicionalmente, A estabelece um novo relacionamento de confiança com o ponto de conexão G, através de algum processo de autenticação aceito pela rede.

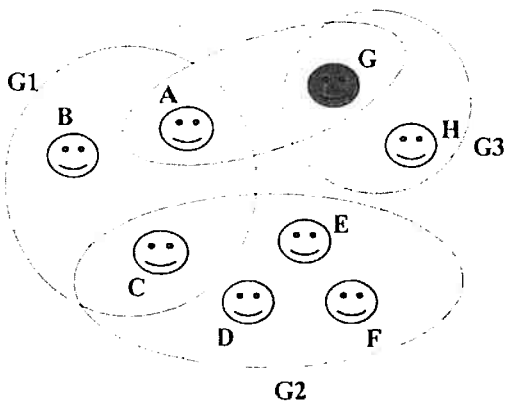


Figura 22: Distribuição de Confiança – 3ª Fase

O nó G envia ao nó A a chave pública assinada (certificada) do nó H dizendo que H é confiável.

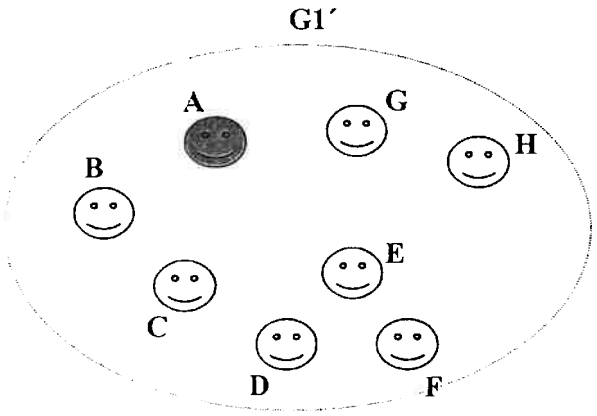


Figura 23: Distribuição de Confiança – 4ª Fase

O nó A divulga para todo rede *Ad hoc* todas as chaves públicas assinadas que ele possui, e uma nova cadeia de confiança é criada, resultando na formação de um novo grupo de confiança G1' que inclui todos os nós da rede.

O processo de distribuição da confiança pode ser utilizado para aprimorar a segurança em protocolos de segurança e roteamento que dependem da distribuição de chaves públicas e permitem a criação de credenciais de confiança. A confiança em uma autoridade certificadora é uma dificuldade porque a confiança está depositada na autoridade central, onde este fator centralizador é contrário aos princípios *ad hoc*.

Ao fazer uso do processo de distribuição de confiança e da técnica de Diffie-Hellman para troca de chaves, é possível se estabelecer uma segurança temporária entre pontos terminais. Eles são, no entanto, vulneráveis a ataques do tipo intermediário, que podem ser de difícil eliminação em ambientes *ad hoc*.

Desta forma, uma álgebra de medidas de confiança precisa fazer parte de qualquer modelo de segurança que pretenda tratar adequadamente as redes Ad-Hoc.

Nesses ambientes de torna clara a necessidade de um processo eficaz de distribuição de confiança sem necessariamente ter que contar com a ajuda de um elemento central único. A questão do estabelecimento das relações de confiança naturalmente se torna um processo probabilísticos nos ambientes Ad-Hoc.

Uma avaliação recíproca das relações de confiança existentes deve ser, de alguma forma, mensurada por alguma grandeza ou conjunto de grandezas estocásticas de forma, a permitir uma modulação (ponderação) no processo de transferência ou distribuição de confiança. Por exemplo, a confiança do nó A em relação ao nó G, quando é transferida para o nó B, ela deve ser ponderada pela confiança existente no nó B em relação ao nó A.

3.13 Modelo de Segurança Java

O modelo de segurança Java é uma das principais características arquitetônicas da linguagem que a tornam uma tecnologia apropriada para ambientes de rede.

A segurança em tais ambientes é importante porque as redes fornecem um caminho potencial para ataques a qualquer computador a elas conectado. A preocupação se torna especialmente forte em um ambiente no qual o software é trazido através da rede e executado localmente, como ocorre com *applets* Java, por exemplo. Como os arquivos de classe para um *applet* são automaticamente carregados quando um usuário acessa o conteúdo de uma página Web com um navegador, é provável que o usuário venha a encontrar *applets* de origem não confiável. Sem nenhuma segurança, este processo seria um modo conveniente para disseminação de vírus.

Conseqüentemente, os mecanismos de segurança Java ajudam a tornar essa linguagem apropriada para redes, visto que eles estabelecem uma confiança mínima necessária nos programas trazidos via rede.

3.13.1 Modelo de Segurança Java 1.0x (modelo original)

O modelo de segurança original é conhecido como modelo "sandbox", que propõe um ambiente restrito para rodar um código não confiável.

O modelo de segurança Java tem como foco proteger o usuário de programas hostis baixados de origens não confiáveis por intermédio da rede. Para cumprir esse objetivo, o Java fornece uma "sandbox" sob medida na qual os programas Java rodam. Um programa Java deve ser executado apenas dentro da sua sandbox. Ele pode fazer o que quiser respeitando esses limites, mas não pode executar nenhuma tarefa fora de seus limites.

A sandbox para applets Java não confiáveis, por exemplo, proíbe muitas atividades, incluindo:

- Ler e gravar no disco local;
- Estabelecer uma conexão de rede com qualquer *host*, exceto o *host* responsável pelo envio do *applet*;
- Criar um processo novo;
- Carregar uma nova biblioteca dinâmica e chamar diretamente um método nativo, dentre outras coisas.

Ao impedir a execução de certas tarefas por programas trazidos remotamente, o modelo de segurança Java protege o usuário da ameaça de códigos hostis.

Por outro lado, as aplicações Java instaladas manualmente no computador do usuário local (*stand-alone*) são consideradas confiáveis, sem restrições de acesso aos dispositivos de sistema.

3.13.2 Modelo de Segurança do Java 1.1x

O modelo original de segurança impedia qualquer applet de utilizar recursos locais no computador do usuário e restringia o destino de conexões de rede.

A versão 1.1 introduz o conceito de applet assinado digitalmente. Um applet assinado digitalmente é tratado como um código local, confiável se a chave de assinatura for confiável para o sistema que recebe o applet.

Um applet assinado é um conjunto de applets na forma de um arquivo Java (JAR) e assinado como uma chave privada. O applet assinado desfruta de acesso ilimitado, de maneira semelhante a uma aplicação local, desde que a chave pública correspondente seja confiável no ambiente de execução local. Applets não assinados são automaticamente tratados como no modelo sandbox.

O modelo de segurança Java 1.1 era menos restritivo do que o modelo sandbox e apresentava um tratamento um pouco mais consistente para applets e aplicações. No entanto, ele possuía uma desvantagem substancial: os applets recebiam acesso irrestrito ou ficavam confinados à sandbox- - não havia opção para acesso seletivo de recursos. Este modelo ilustrou um outro exemplo de implementação inflexível, na qual a política era forçada pelo mecanismo.

3.13.3 Modelo de Segurança do Java 2

O modelo de segurança Java 2, como mostra a Figura 24, possibilita uma política consistente e flexível para applets e aplicativos. Embora aplicativos ainda rodem sem restrições por default, podem estar sujeitos às mesmas políticas dos applets.

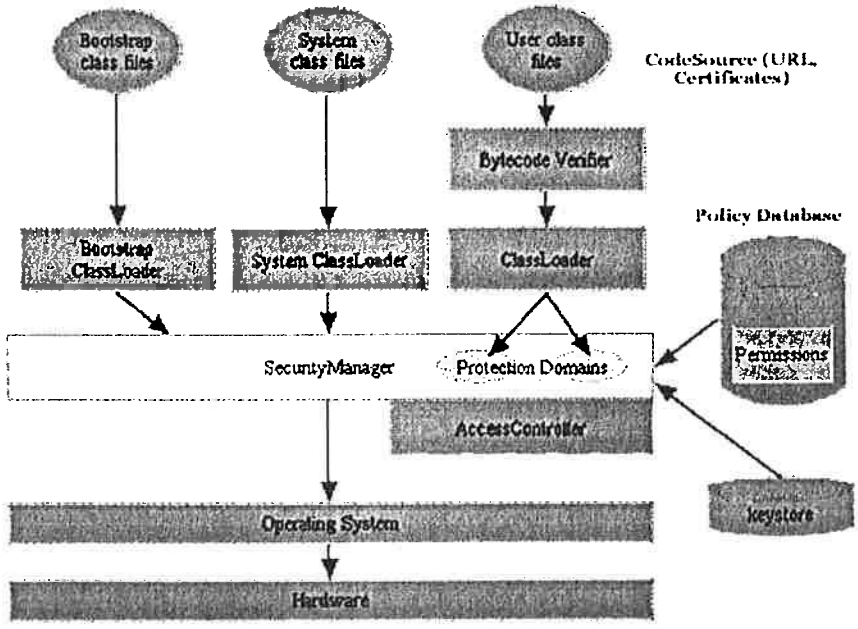


Figura 24: Java 2 Security Architecture

Arquitetura de Segurança Java 2

O modelo Java 2 também introduz o conceito de Domínio de Proteção, o qual permite uma política de segurança altamente flexível, independente de sua implementação.

Um domínio de proteção é formado por um código fonte e pelas permissões de acesso aos aplicativos do código fonte [OAKS98]. Um domínio de proteção é o conjunto de políticas de segurança e de definições de área de atuação.[MDOY98]. O código fonte é definido pela sua origem (a URL da qual o código foi obtido) e pelo responsável (que é denominado *principal* na especificação), identificado pela entidade que assina o código.

A política de segurança é definida pelo usuário ou pelo administrador do sistema. As verificações de segurança são feitas pelos aplicativos locais, assim como pelos applets.

Na Figura 25 é apresentada a evolução do modelo Java de segurança.

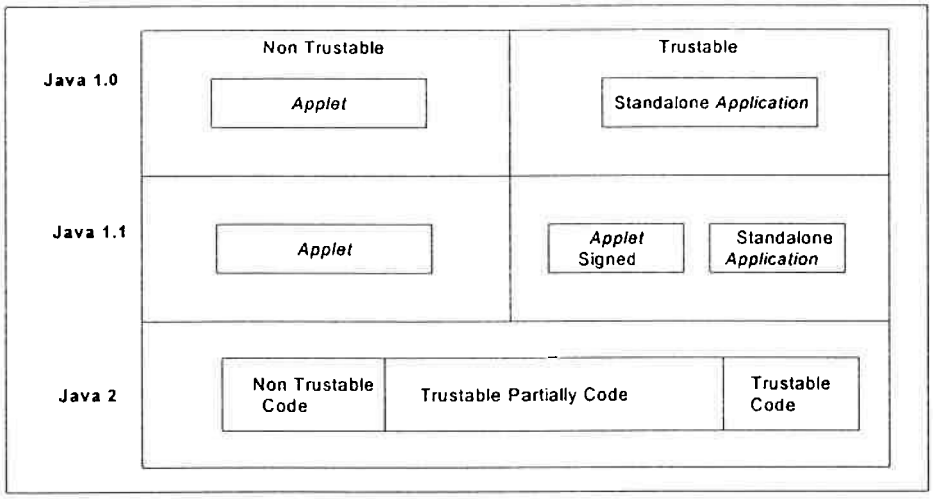


Figura 25: Comparação entre as diferentes versões do modelo de segurança Java

4 Modelo de segurança para redes Ad-Hoc

Este capítulo descreve o modelo de segurança para redes Ad-Hoc baseado nas discussões desenvolvidas no capítulo anterior, onde se demonstrou que, principalmente devido as características dinâmicas associadas as redes Ad-Hoc, os modelos tradicionais de segurança não apresentam uma solução adequada para o desenvolvimento de aplicações seguras nesse ambiente.

Mesmo com todos os mecanismos já existentes nas tecnologias de redes sem fio presentemente utilizadas (IEEE 802.11 e Bleutooh) esses modelos possuem limitações que restringem a sua eficácia somente à camada física. Apesar dessas limitações, esses mecanismos são essenciais para a segurança total dessas redes. O que se deve fazer é complementa-los com outros mecanismos que venham a ser definidos em níveis mais altos da rede.

Dentre as características mais importantes que devem ser cobertas pelo novo modelo sendo proposto destacam-se:

- A hierarquia de confiança não deve depender exclusivamente de um único nó central;
- O modelo deve apresentar solução de proteção para todos componentes inteligentes (com capacidade de processamento) da rede, pois não existirá um único ponto de entrada nessa rede;
- O conceito de confiança deve ser criado ou estabelecido a partir de condições iniciais ("set-up") e pode ser alterado/aprimorado dinamicamente baseado no comportamento dos nós da rede durante a operação da mesma;
- Deve-se definir uma maneira pragmática de se avaliar as relações de confiança baseado num processo inicial de autenticação;
- O modelo deve prover mecanismos de autenticação mútua entre nós usuários e nós provedores de serviços;
- O modelo deve se basear, na medida do possível, no modelo de segurança Java versão 2, para manter compatibilidade ou mesmo poder utilizar os resultados positivos já alcançados e que forem aplicáveis ao ambiente de redes Ad-Hoc;
- O modelo deve tratar adequadamente os visitantes desejados e implacavelmente os intrusos, procurando definir um compromisso equilibrado entre flexibilidade de utilização e segurança;
- O modelo deve captar e poder lidar adequadamente com a natureza dinâmica, móvel e mutante dos nós das redes Ad-Hoc, reagindo coerentemente nas situações inusitadas naturalmente provocadas por esse dinamismo;
- O modelo de segurança deve focalizar preferencialmente o conceito de prestação de serviços (redes de serviços) pois é através desse conceito que se atinge ou se atende as necessidades dos nós usuários das redes Ad-Hoc;

- O modelo não deve impedir a participação de dispositivos simples e não inteligentes, com um nível de segurança compatível com suas capacidades e sem comprometer a segurança da rede como um todo;
- As relações de confiança devem poder ser aplicáveis em diversos níveis de granularidade e de forma totalmente seletiva para compatibilizar a natureza diversa e dinâmica dos nós participantes das redes Ad-Hoc.

Abaixo descreve-se um modelo de segurança de alto nível, para uma rede de serviço, utilizando a infra-estrutura ad hoc. Diversos conceitos utilizados podem ser também aplicáveis as redes tradicionais.

Inicia-se esta descrição com a identificação das entidades que compõem o modelo seguindo-se a descrição das relações existentes entre elas.

4.1 REDES DE SERVIÇO

Nas redes de serviço, ofertas e solicitações de serviços interagem através da infra-estrutura de comunicação. A infra-estrutura de comunicação da rede ad hoc sem fio é composta por dispositivos sem fios, os quais se comunicam de uma maneira dinâmica, sem qualquer infra-estrutura fixa.

Uma rede de serviços é composta por uma infra-estrutura de comunicação e seus componentes, que seriam as entidades que participam do processo de oferta e solicitação de serviços.

Um rede de serviços sem fio é um sistema que utiliza como meio de comunicação uma rede ad hoc sem fio.

4.1.1 Entidades

As entidades que compõem essa rede podem ser classificadas em **usuários, provedores de serviço (ou simplesmente provedores)** e **dispositivos.** Todas as entidades podem ser incluídas em um processo de identificação, fato este que se torna essencial, se levarmos em conta a grande importância da proteção do sistema contra entidades ilegítimas. Considerando seu comportamento dinâmico, as entidades podem estar presentes ou ausentes, dependendo da posição no raio de alcance da rede , assim como da condição ligado/desligado das mesmas.

As entidades podem ser também classificadas de acordo com sua natureza, física ou lógica. **Entidades físicas** são equipamentos com as mais diversas complexidades. Os aparelhos mais simples podem ter somente uma função, tal como condicionadores de ar, forno de microondas, etc. Os mais sofisticados oferecem múltiplos serviços, tais como: os telefones sem fio com funções de PABX, secretárias-eletrônicas e acesso à Internet; computadores que se comunicam com aparelhos sem fio, etc.

Entidades lógicas precisam ser hospedadas por entidades físicas para que possam existir. As entidades lógicas são instâncias de processos que rodam em

servidores ou dispositivos de acesso, incluindo aí também, os processos que interagem com os usuários finais dos serviços da redes.

• Usuários

Os usuários são entidades lógicas que solicitam serviços aos provedores de serviços da rede. Eles utilizam os serviços da rede e têm propriedade de serem identificados.

• Provedores de Serviço

Os provedores de serviços são entidades lógicas com capacidade, funcionalidade e disponibilidade para responder às solicitações de serviços que lhe são apresentadas. A capacidade de serviço corresponde ao grau de intensidade com a qual um serviço pode ser fornecido. A amplitude dessa capacidade está relacionada à quantidade de recursos alocada ou associada ao serviço. A funcionalidade está relacionada à habilidade em fornecer, suprir ou desempenhar um conjunto de funções, e a disponibilidade relaciona-se aos períodos de tempo durante os quais o entidade é capaz de desempenhar seus serviços funcionais.

Um provedor de serviços também pode solicitar serviços a outras entidades, assim como também tem a propriedade de serem adequadamente identificados.

• Dispositivos

Os dispositivos são entidades físicas, capazes de hospedar os serviços e usuários. Os dispositivos oferecem, usualmente, uma interface para o usuário, como visores, teclados, microfones e *touch screens*. Esses dispositivos têm endereços físicos e podem ser identificados.

Alguns dispositivos fornecem serviços nativos, para os quais foram especialmente concebidos. Esse tipo de dispositivo é chamado dispositivo-fim e está associado a um ou mais serviço-fim. Exemplos destes dispositivos são uma impressora, um condicionador de ar, etc.

Outros dispositivos são usados como agentes intermediários, possibilitando o acesso aos serviços-fim. Este tipo de dispositivo é denominado dispositivo-meio ou dispositivo de acesso. Exemplos desses dispositivos são os roteadores, os controles-remotos, etc. Existem entidade que podem assumir tanto as funções de dispositivos-fim como de acesso.

Os dispositivos podem estar **presentes** ou **ausentes**, dependendo da posição no raio de alcance da rede e da condição ligado/desligado.

Os dispositivos também podem ser classificados como **permanente** ou **visitante.** Os dispositivos permanentes são aqueles que têm privilégios duráveis no contexto de uma rede AD HOC. Estes privilégios são definidos por um processo de configuração inicial. Os dispositivos visitantes são aqueles que estão no raio de alcance da rede, são capazes de comunicar-se com ela e não possuem privilégios duráveis. Os visitantes podem ser classificados como não identificados, enquanto não submetidos a um processo de identificação/autenticação, e como identificados quando tiverem passado por um processo positivo de identificação e autenticação.

Os visitantes, que tiverem passado por um processo de identificação, podem assumir identidades genéricas (anônimos) ou específicas (visitantes identificados).

A relação entre os diferentes tipos de entidades pode ser vista na Figura 26.

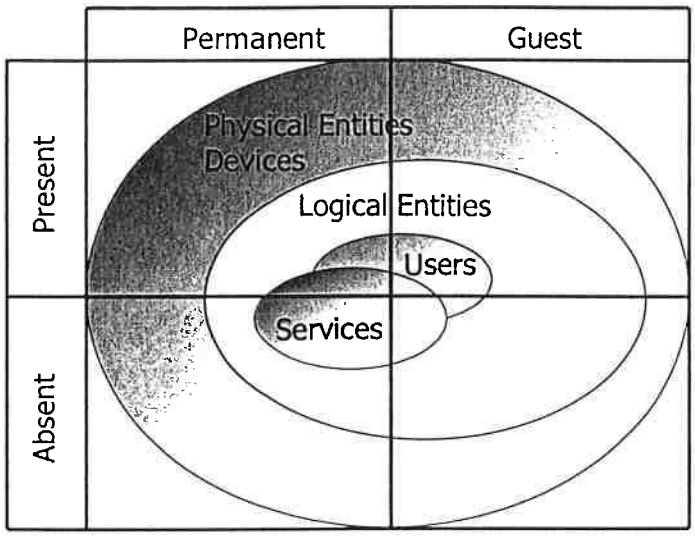


Figura 26: Relação entre os diferentes tipos de entidades

Como resultado do processo de autenticação atribui-se uma medida de confiança ao dispositivo autenticado. Esta medida poderá variar no tempo em função do comportamento da entidade operando na rede. Esta medida indicadora de confiança pode ser transitivamente passada de um nó para outro, criando assim, um processo de distribuição de confiança.

4.1.2 Infra-estrutura de Comunicação

A infra-estrutura de comunicação idealizada pelo modelo de segurança possibilita a troca transparente de dados entre entidades. Não se requer tecnologia especial para o serviço de rede. As redes ad hoc, porém, serão tidas como certas neste contexto.

4.2 Autenticação e autorização

Antes que um serviço ou função possa ser usado por uma entidade, uma verificação das permissões adequadas para esse acesso deve ser efetuada. Primeiramente, a entidade é identificada com o objetivo de se verificar se ela é realmente quem diz ser. Este processo é chamado de **autenticação.** Posteriormente, confronta-se o conjunto de permissões associados a esta entidade com as requisições de serviço por ela emitidas. Este processo é chamado de **autorização**.

As entidades são classificadas, na rede, através do resultado do processo inicial de autenticação, que se denomina registro. Esta classificação pode depender de configurações pré-estabelecidas e ocasiona a emissão de um ou mais certificados digitais que, por sua vez, definem indiretamente os direitos de atuação (permissões) da entidade.

Denominam-se **Ações** as iniciativas individuais das entidades, sob a forma de solicitações ou respostas. Dispositivos de acesso, em geral, executam as solicitações de serviço e recebem respostas. Dispositivos que hospedam provedores

de serviço executam as ações decorrentes das solicitações de serviço, retornando as respostas (e/ou resultados).

Denominam-se **Permissões** os direitos à execução de ações. As permissões podem ter diferentes granularidades. As permissões de serviço definem os direitos ao uso de um serviço como um todo, enquanto permissões funcionais (ou operacionais) definem os direitos à ação em funções específicas daquele serviço.

Um mapeamento eficiente, englobando serviços e entidades, é uma necessidade para que a permissão possa ser verificada e controlada eficientemente. Um mapeamento direto e individual, que englobe serviços e entidades pode tornar-se impraticável em redes com muitos usuários ou serviços complexos. O modelo atual proposto utiliza a noção de grupos e de perfis.

Grupos são conjuntos de entidades. Os grupos são criados com base nas características ou objetivos comuns às entidades a ele pertencentes.

Perfis definem conjunto de permissões, as quais podem estar relacionadas aos dispositivos, serviços ou funções. Os perfis constituem uma maneira adequada para agrupar permissões e, posteriormente, serem mapeados aos grupos de entidades.

4.2.1 Grupos e perfis

Os grupos são usados para classificar entidades, de acordo com algum critério, ou, simplesmente, para permitir que diferentes direitos de acesso sejam conferidos a seus componentes.

Em redes simples, como a formada entre um controle remoto e o aparelho ao qual ele controla, um só grupo pode ser suficiente. O direito de acesso deste grupo pode resultar em direitos totais de acesso, por parte do controle remoto, em relação ao aparelho por ele controlado.

Em redes de complexidade média, poucos grupos básicos podem ser necessários. Tomando-se como exemplo o ambiente doméstico, pode-se definir os seguintes grupos:

- Pais
- Filhos
- Empregados
- Outros

Os pais podem ter acesso e controle total sobre todos os dispositivos da rede. Os filhos podem ter acesso a todos os dispositivos (e, assim, ao conjunto completo ou parcial dos serviços que eles oferecem), mas não devem efetuar configurações. Os empregados devem ter acesso a um grupo mais reduzido de dispositivos, com

permissões de uso mais restritas. O grupo **outros** é pré-definido e serão atribuídos a entidades ainda não identificadas (reconhecidas e autenticadas) pelos dispositivos da rede.

Continuando nosso exemplo doméstico, suponhamos que a rede seja formada por um telefone e seus fones de ouvido sem fio. O telefone e os fones de ouvido serão capazes de identificar os usuários, através das impressões digitais, senhas ou outro mecanismo de identificação.

Pais e filhos terão os direitos acima descritos. Os empregados poderão receber algumas chamadas, mas a eles somente será permitido efetuar ligações para números pré-estabelecidos (ex.: celulares dos pais).

Quatro perfis podem ser definidos para mapear essa situação:

- Administrador
- Usuário
- Restrito
- Outros

A Tabela 4 demonstra o mapeamento englobando perfis e ações.

Tabela 4: Example of mapping between profiles and actions

Ação	Perfil			
	Administrador	Usuário	Restrito	Outros
Receber chamadas	✓	✓	✓	✓
Realizar chamadas	✓	✓		
Realizar chamadas com atributo: número destino 123-3456 (celular dos pais)	✓	✓	✓	
Realizar chamadas com atributo: número destino 911 (emergência)	✓	✓	✓	✓
Configuração	✓			

A ação "Realizar chamadas" tem uma forma geral e mais duas específicas. A forma geral garante total acesso para realizar chamadas. As duas específicas têm um número de telefone como atributo e somente permitem chamadas para esses números.

Agora, cada grupo necessita ser associado a esses perfis. Esta associação é apresentada na

Tabela 5.

Tabela 5: Exemplo da associação entre perfis e grupos

Grupo	Perfil
Pais	Administrador, Usuário
Filhos	User
Empregados	Restricted
Outros	Outros

Concluindo, o mapeamento englobando usuários (entidades) e grupos é apresentado na Tabela 6.

Tabela 6: Exemplo do mapeamento englobando usuários e grupos

Usuário	Grupo
George, Jane	Pais
Elroy, Judy	Filhos
Rosie	Empregados
Spacely	Outros

As tabelas apresentadas acima estabelecem os direitos de acesso para cada entidade.

Os direitos de acesso são definidos como a relação que estabelece o direito de uma entidade de executar uma dada ação. Os direitos de acesso são definidos, de uma forma prática, e podem ser verificados através do mapeamento englobando usuários, grupos, perfis e ações.

$$\text{Entidade} \Leftrightarrow \text{Grupo} \Leftrightarrow \text{Perfil} \Leftrightarrow \text{Ação}$$

O **raio de ação** de uma entidade é definido por todas as ações que ela tem o direito de executar.

Os direitos de acesso que um serviço de rede confere a uma entidade são proporcionais ao nível de confiança que ele e sua rede tem a respeito dessa entidade. O nível de confiança indica até que ponto o serviço de rede confia em uma entidade. O nível de confiança pode ser alterado, a qualquer tempo, através da intervenção do administrador (introdução de um novo dispositivo na rede), ou como resultado do comportamento operacional da entidade, portanto resultando na promoção, no rebaixamento ou na eliminação desse elemento nas relações de confiança existentes. Concluindo, o nível de confiança pode ser automaticamente alterado, através da autenticação, como no caso de uma entidade passar do estado de não identificada para o de identificada ou pelo resultado de suas ações operacionais face aos serviços e usuários da rede.

A autenticação de uma entidade pode ser feita através de várias etapas, dependendo do serviço requisitado. Os serviços públicos da rede podem não precisar de autenticação, enquanto que os serviços críticos, tais como assinatura de documento ou transações comerciais, sendo executados através de dispositivos domésticos, podem requerer múltiplos níveis de identificação e autenticação. O serviço pode solicitar identificações apropriadas, de acordo com seu próprio critério, na ordem e quantidade desejadas, permitindo grande flexibilidade e aumentando a segurança da operação. Vários mecanismo de autenticação podem ser utilizados, tais como, métodos baseado em senhas, *tokens*, certidões, informações cadastrais e comportamentais e características biométricas.

Após o estabelecimento de sessão, onde foi exigida a autenticação mútua dos dispositivos, solicitações adicionais de identificação podem ser opcionalmente trocadas. A identificação mútua inicial procura empregar uma quantidade mínima de informações necessárias para que a privacidade da entidade não seja comprometida. Se alguma das entidades (o usuário ou o serviço) sentir necessidade de autenticação adicional, isto deve ser feito através de uma nova e específica etapa de identificação. Dependendo das respostas obtidas, novas solicitações podem ser emitidas até que se chegue à emissão de uma mensagem garantindo ou negando a execução da ação desejada.

4.3 Segurança das Aplicações

Muitos dispositivos, como notebooks ou computadores portáteis, suportam a instalação, configuração e execução de aplicativos. Estas atividades constituem um potencial de risco em termos de segurança, porque podem permitir a execução de códigos maliciosos, a proliferação de vírus, comprometer a privacidade, entre outros.

Com a finalidade de proteção contra atividades potencialmente inseguras, é proposto um modelo de segurança, similar ao Java versão 2, que deverá apresentar as seguintes características:

- Estar seguro com relação a aplicativos mal-intencionados: são necessários programas preventivos para que o ambiente do computador não seja danificado. Vírus e cavalos de Tróia são exemplos desses programas;
- Proteger contra programas invasores: é necessário evitar que informações privadas no dispositivo hospedeiro sejam acessadas ou abertas por esses programas;
- Suporte a auditoria: a identidade do autor e do usuário do programa deve ser registrada em log;
- Usar criptografia: todos os dados sensíveis em trânsito, isto é, enviados ou recebidos de/para a rede ou para dispositivos de armazenamento (por exemplo, discos rígidos e banco de dados), devem ser criptografados;
- Auditorias de suporte: todas as operações potencialmente confidenciais devem ser registradas;
- Estar bem definido: uma especificação de boa qualidade sobre segurança deve ser definida e seguida rigidamente;

- Ter possibilidades de verificações: regras de operação devem ser estabelecidas e sua observância verificada;
- Garantir um bom comportamento por parte dos aplicativos: deve haver prevenção no sentido de que os programas não consumam excessivos recursos do sistema, tais como CPU, memória e armazenamento secundário.

Um vírus não deve ser um aplicativo reconhecido pelo dispositivo porque ele não possui uma assinatura digital válida , e conseqüentemente deve ser impedido de executar.

Quando um aplicativo necessita de mais privilégios, ele precisa necessariamente passar a ser membro de um grupo que possua esses privilégios através de algum processo adicional de autenticação, ou um usuário autorizado com poder de administrador precisa modificar as permissões do sistema.

4.4 Serviço de Registro

O objetivo do serviço de registro é documentar a existência de novas entidades na rede de serviços (i.e., inicialmente autenticando-as na rede), emitindo certificados assinados digitalmente para as mesmas. Tais certificados devem ser apresentados por entidades usuárias em cada pedido de serviço com propósitos de autenticação. Se o certificado for autêntico e válido e após um processo de desafio-resposta, o provedor de serviços utiliza-o para verificar os direitos de acesso relacionados ao usuário final identificado.

Para utilizar o serviço de localização ("lookup") (que pertence à infra-estrutura básica de uma rede baseada em serviços, e contém uma lista de serviços disponíveis), assim como os serviços gerais, uma entidade deve identificar-se utilizando os certificados emitidos pelo serviço de registro, denominado autoridade de registro.

O serviço de registro e o serviço de localização poderiam estar associados, mas não coexistem necessariamente no mesmo dispositivo. Ambos os serviços são essenciais à rede, mas o modelo de segurança não exige que eles estejam disponíveis o tempo todo.

O serviço de registro é obrigatório ao modelo de segurança e, como todos os serviços em uma rede ad hoc, não está fixo em um dispositivo e pode existir em qualquer dispositivo da rede capaz, permanente e previamente identificado. Esses dispositivos poderiam estar em uma das possíveis autoridades de registro; essas entidades devem ser reconhecidas entre seus pares da rede.

As autoridades de registro controlam um banco de dados móvel das entidades registradas, denominado registro. Deve ser distribuído e dividido entre os dispositivos permanentes com capacidade para serem autoridades de registro. Os provedores de serviço devem aceitar os certificados assinados pelas autoridades de registro da rede.

Uma entrada no registro é indexada através de um identificador único associado a cada entidade (por exemplo, uma combinação do endereço físico do dispositivo e um PIN do dispositivo). Inclui informação sobre a certificação de entidades (por exemplo, a chave pública de uma entidade) e, para dispositivos, informação sobre a classe a que ele pertence (visitante, permanente ou identificado).

Quando dispositivos são registrados eles são inicialmente classificados como visitantes anônimos, visitantes identificados ou permanentes. O serviço de registro classifica os dispositivos baseados em uma lista pré-configurada de dispositivos que deve pertencer a uma classe específica (por exemplo, a lista de dispositivos permanentes) assim como em regras para classificação automática (i.e., se um dispositivo está de acordo com alguns requisitos, ele pode ser classificado automaticamente e registrado). O serviço de registro também pode requerer intervenção manual para classificar algum dispositivo.

Dispositivos visitantes, quando registrados, geralmente recebem certificados de curta duração. A autoridade de registro deve ter um controle de tempo para esse tipo de acesso, e deve limitar o número de dispositivos visitantes anônimos ao mesmo tempo.

Após um período de tempo afastado de sua rede permanente, um dispositivo deve ser capaz de reconhecer sua rede através de sua identificação lógica de registro. Essa identificação lógica deve ser mudada periodicamente, seguindo uma seqüência pseudo-aleatória gerada de uma semente distribuída para dispositivos permanentes. Se o sigilo da semente estiver comprometido, o mesmo pode ser alterado pelo serviço de registro ativo e propagado pela rede ad hoc. Dispositivos fora da área da rede permanente terão que ser submetidos a um novo registro. Esse método garante a privacidade do usuário, evitando o rastreamento do dispositivo e a privacidade do serviço da rede, evitando a identificação a um usuário não-autorizado.

O serviço de registro também tem uma lista de revogação de certificados. Essa lista contém os certificados revogados e cada um deles deve estar na lista pelo menos até que o certificado expire.

Um provedor de serviços também pode emitir certificados digitais assinados, independentemente de uma autoridade central de registro. Nesse caso, esses certificados autenticam as entidades somente para os serviços fornecidos pelo provedor emissor de serviços, que se torna um exemplo especial de uma autoridade de registro restrita a serviços específicos. Quando combinada com mecanismos de distribuição de confiança, um conjunto de tais autoridades especiais de registro pode assumir o papel completo de uma autoridade central de registro.

4.5 Comportamento Dinâmico

Tendo em vista o processo dinâmico de inserir um dispositivo em um ambiente de rede ad hoc, devemos considerar como esse dispositivo se comporta nesse ambiente. Como visto anteriormente, quando os dispositivos são registrados na rede, eles são classificados como visitantes anônimos, visitantes identificados ou permanentes.. Figura 27 mostra a máquina de estado finito relacionada ao comportamento do dispositivo.

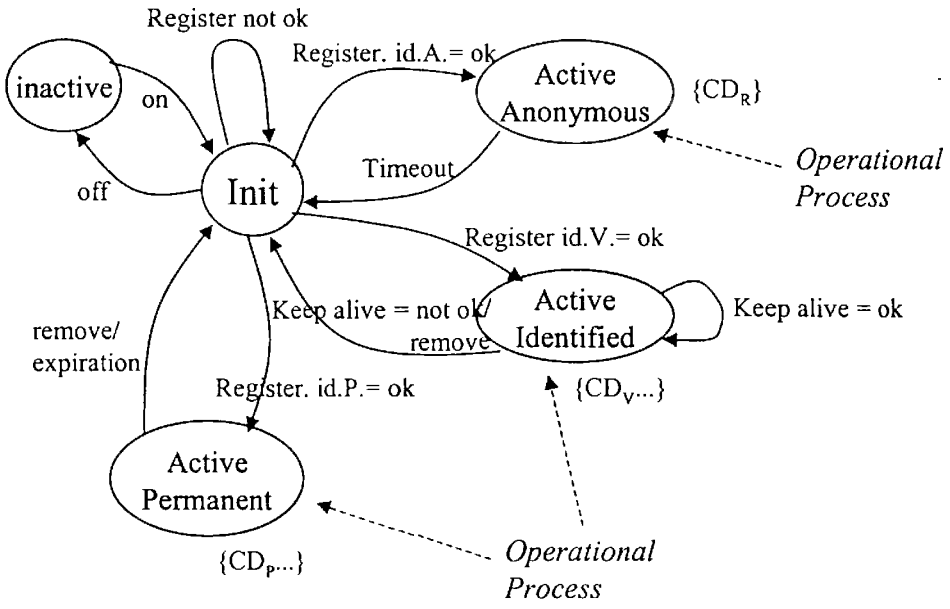


Figura 27: Máquina de Estados para o Acesso dos Dispositivos da Rede

Quando um dispositivo acessa a rede pela primeira vez, ele entra em um estado inicial (Init), no qual é um visitante não-identificado. Se for registrado com sucesso junto ao serviço de registro, torna-se um membro da rede e muda para um estado ativo, dependendo da classificação que receber do serviço de registro (Visitante Permanente, Identificado ou Visitante Anônimo). Permanece no estado inicial enquanto não for registrado com sucesso.

Se o dispositivo for desligado ou deixar o ambiente de rede, ele deixa o estado inicial e vai para um estado inativo.

Se o dispositivo for registrado como permanente, significa que ele tem privilégios duráveis na rede. Ele deixa o estado permanente quando seu certificado expira ou é revogado (i.e., é removido da lista de dispositivos permanentes no serviço de registro).

Quando um dispositivo recebe um certificado de visitante anônimo, de curta duração, ele tem um período pré-definido para acessar serviços públicos de rede (aqueles que não precisam de uma identificação), retornando ao estado inicial quando acaba o tempo.

E finalmente, se o dispositivo for um visitante identificado, ele pode acessar qualquer rede de serviços públicos; como ele é identificado, pode ter mais privilégios do que o dispositivo-visitante anônimo. Ele retorna ao estado inicial quando é removido, quando seu certificado expira ou quando o mecanismo de controle do tipo keep-alive detecta que ele não está mais ativo.

Quando um dispositivo está em um dos estados ativos, é necessário considerar seu comportamento quando um serviço é solicitado, conforme mostrado na Figura 28.

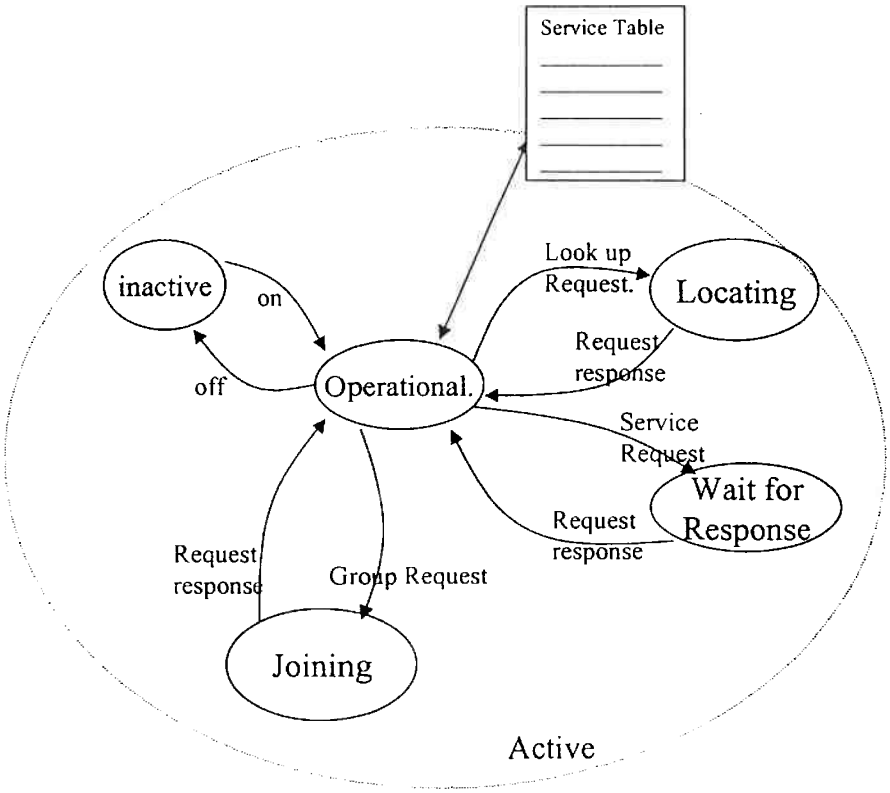


Figura 28: Máquina de estado finito de acesso a serviços

No momento em que o dispositivo estiver em um estado ativo, ele pode solicitar uma localização de serviço ou um registro de grupo para juntar-se a grupos adicionais de modo a ganhar privilégios adicionais. A resposta de um pedido indica se o mesmo foi bem-sucedido e, em caso negativo, o status do erro de acordo com uma tabela de erros.

Antes de utilizar um serviço, o dispositivo precisa encontrá-lo. Através do protocolo de localização de serviços, ele solicita uma localização de serviços, passando para o estado de localização ("Locating"). Ele retorna ao estado ativo após receber a resposta. Quando um dispositivo estiver no estado ativo enquanto visitante anônimo, só poderá localizar serviços públicos.

Quando solicita um serviço, entra no estado de espera por resposta ("Waiting for Response") e sai dele quando recebe a resposta do provedor de serviços.

4.5.1 Distribuição de confiança

Uma vez passado com sucesso por um processo de autenticação, provavelmente executado por um serviço de registro, a entidade entrante na rede recebe uma classificação caracterizada por um dos estados mostrados na figura 27. Essa atribuição de estado corresponde a uma medida de confiança que a rede atribui a essa entidade. O valor dessa medida é função do resultado do processo de autenticação.

Toda entidade ao encerrar o seu processo de autenticação recebe uma atribuição de confiança representada por uma dupla (mc, md) onde mc representa o grau de confiança, que varia de 0 a 1, e md representa o grau de desconfiança atribuídos a

essa entidade. É importante notar que essas grandezas não são complementares e não devem necessariamente somar 1, pois pode existir também a situação onde não se tem informações nem para se confiar e nem para se desconfiar da entidade.

Essa medida composta de confiança/desconfiança associada a um par de entidade pode variar à medida que ela começa a interagir e atuar na rede e conseqüentemente, através de seu comportamento pode-se obter mais informações sobre a mesma a ponto de diminuir a incerteza sobre essa relação de confiança/desconfiança.

O valor inicial dessa atribuição de confiança depende do mecanismo específico de autenticação a que a entidade foi submetida, das informações por ela prestadas durante esse processo e das credenciais ou recomendações por ela trazidas para a autenticação.

Outra forma dessa grandeza poder variar é quando, através de uma relação de transitividade, a confiança/desconfiança é transferida através de uma cadeia de nós da rede.

De posse de seu nível de confiança uma entidade pode se apresentar a um provedor de serviços fazendo requisições de uso. O processo de autorização deve levar em conta o nível de confiança **mc** e o de desconfiança **md**, confrontando-os com o nível mínimo (**nmc**) de confiança exigido e pelo nível máximo de desconfiança (**nmd**) tolerado pelo serviço requisitado. Somente quando estes dois testes forem positivos é que a entidade teria permissão de uso do serviço requisitado, ou seja:

$$\textbf{condição de permissão} = (\ mc \geq nmc) \text{ e } (md \leq nmd)$$

Na situação de distribuição de confiança quando o nó A atribui ao nó B o par $(mc_b, md_b)_A$ e o nó B atribui ao nó C o par $(mc_c, md_c)_B$, o modelo de distribuição estabelece que a confiança/desconfiança do nó A em relação ao C, deve ser determinado por uma função que combine adequadamente essas duas medidas. Existem várias funções disponíveis na literatura que poderiam ser utilizadas neste caso. Uma delas é baseada na teoria de Dempster-Shafer [GINS84].

4.6 Mecanismos de Segurança

O modelo de segurança engloba vários mecanismos de segurança, os quais são utilizados pelas entidades para interagir entre si de forma segura. Os principais mecanismos de segurança estão descritos nos itens a seguir.

4.6.1 Descoberta da Rede

Uma entidade pode pertencer a diferentes redes (por exemplo, uma rede doméstica e uma rede corporativa). Antes de acessar um serviço, a entidade deve descobrir em qual rede ela se encontra (pela identificação do registro, por exemplo) e selecionar as credenciais e os certificados apropriados para os serviços de rede. Essa tarefa está sob a responsabilidade do mecanismo de descoberta da rede (localização).

4.6.2 Registro Individual

Para acessar um serviço da rede, uma entidade precisa passar por um processo de registro individual: qualquer entidade nova na rede deve se registrar junto ao serviço de registro. O serviço de registro, de acordo com sua configuração, fornece à entidade registrante um certificado especial, denominado certificado individual após a execução bem sucedida de um processo de autenticação. O certificado individual é válido para aquela rede específica e identifica corretamente a entidade quando ela se apresenta diante de um serviço da rede.

4.6.3 Registro de Grupos

Conforme visto anteriormente, as entidades podem pertencer a um ou mais grupos e, dependendo dos grupos aos quais ela pertence, as requisições de serviço podem ser concedidas ou negadas. Para associar-se a um grupo, a entidade deve executar um processo de registro de grupo: ela se registra a grupos específicos junto ao serviço de registro. Como resultado do registro de grupo, a entidade recebe credenciais de membro do grupo, que devem ser usadas para provar aos serviços a que grupos ela pertence.

Durante o registro individual, a autoridade de registro pode automaticamente fornecer credenciais de membro juntamente com o certificado individual, dependendo da configuração.

4.6.4 Configuração de Serviço de Registro

Para que as entidades se registrem com sucesso e recebam certificados individuais e de grupos, o serviço de registro deve ser configurado. O mecanismo de configuração do serviço de registro é responsável pela definição das regras que devem ser utilizadas no processo de registro a fim de emitir certificados individuais para visitante permanente, visitante identificado ou anônimo. Como um exemplo dessas regras, há a lista de entidades que devem receber certificado de usuário permanente ou visitante identificado, ou os requisitos que as entidades devem ter para receber um certificado de visitante identificado ou anônimo. Esse mecanismo também é responsável pelo gerenciamento de grupos, permitindo a criação e a remoção de grupos, assim como a configuração de membros de grupos.

4.6.5 Configuração do Serviço

Cada serviço deve ser configurado a fim de que se tenha uma comunicação segura. Esse mecanismo é responsável pela configuração de parâmetros de segurança em um serviço, tais como os direitos de acesso relacionados aos grupos, entidades individuais e perfis de operação, assim como os requerimentos de segurança para o serviço. Toda a configuração deve ser assinada, para fins de auditoria.

É possível que um serviço emita certificados especiais para identificar entidades que tenham acesso permitido às funções, independentemente da autoridade de registro. Esses certificados são gerenciados através da configuração do serviço.

A funcionalidade de um dispositivo pode ser aumentada com a adição de novos serviços. Como tais serviços podem ser instalados via rede, podem estar sujeitos a

cavalos de Tróia ou vírus. O mecanismo de configuração do serviço é responsável pela verificação da integridade do novo serviço e pelos recursos a que esse novo serviço pode ter acesso, dependendo de seu código binário (por exemplo, se é digitalmente assinado por uma empresa ou por um usuário da rede ou se não está assinado), e do usuário responsável pela instalação do serviço. Além disso, o mecanismo de configuração é utilizado para definir como esse novo serviço pode interagir com outras entidades e com os dispositivos em que elas estão sendo hospedadas.

4.6.6 Autenticação

Um mecanismo importante na infra-estrutura de segurança é a identificação de entidades, tais como usuários, dispositivos ou serviços. Essa identificação é possível através dos certificados individuais, que são emitidos e assinados pela autoridade de registro. Para se identificar em uma rede, uma entidade apresenta seu certificado individual, emitido pela autoridade de registro daquela rede. Às vezes, também é necessário que uma entidade se identifique como membro de grupos privilegiados; nesse caso, a entidade deve apresentar uma credencial de membro do grupo para poder provar que faz parte dele.

O mecanismo de autenticação é responsável pelas identificações necessárias para a comunicação segura. Pode envolver vários passos; por exemplo, um serviço pode solicitar, além da identificação do dispositivo, a identificação do usuário que está operando o dispositivo. Além disso, também pode ser necessário que o serviço se identifique ao dispositivo requerente ou ao usuário requerente, a fim de evitar serviços falsos (identificação mútua).

4.6.7 Estabelecimento de Sessão

Quando uma entidade quiser se comunicar com um provedor de serviços, ela deve estabelecer uma sessão entre eles. Uma sessão deve fornecer um túnel criptografado para as comunicações no meio sem fio, para assegurar a confidencialidade e a integridade necessárias para a comunicação segura.

Durante o estabelecimento da sessão, há a fase de autenticação, em que a entidade prova sua identidade ao provedor de serviços e vice-versa (se necessário). Uma vez estabelecida a sessão, a entidade pode emitir requisições de serviço e, dependendo da configuração de serviço, a entidade pode precisar fornecer credenciais de membros de grupo adicionais para ter a requisição específica autorizada. A fase de autenticação também pode ocorrer durante a sessão se alguma das entidades envolvidas na comunicação acreditar que haja um problema de segurança.

4.6.8 Serviço de Log

A rede pode fornecer um serviço de log para garantir o não-repúdio e a auditoria. Deve haver log para operações críticas de segurança, tais como registros individuais e de grupo e configuração de serviço de registro. Os serviços podem também usar um mecanismo de log para armazenar e notificar outras entidades sobre eventos de segurança, tais como a configuração de serviço de segurança e a tentativa de usar certificados e credenciais revogados.

4.6.9 Revogação de Certificado e Credenciais

Quando grupos ou entidades são removidas da rede, os certificados individuais e as credenciais de grupo devem ser revogadas. O mecanismo de revogação é responsável pela manutenção e divulgação da lista de certificados e credenciais revogados. Ele permite aos serviços de segurança crítica uma forma de verificar instantaneamente se as credenciais e certificados são ainda válidos assim como permite que os serviços recebam periodicamente as listas.

4.6.10 Filtragem de Conteúdo

O mecanismo de filtragem de conteúdo é responsável por evitar que vírus e outros códigos maliciosos não entrem em uma unidade e corrompam os serviços. Por exemplo, ele deve verificar novos serviços ou arquivos quando estiverem sendo baixados em uma unidade bem como os e-mails com arquivos anexados.

4.6.11 Verificação em Tempo de Execução

Os processos que implementam os serviços devem ser executados em um ambiente restrito, com códigos assinados e não assinados possuindo diferentes restrições. Se um código malicioso atravessa o mecanismo de filtragem de conteúdo, o mecanismo de verificação em tempo de execução deverá detectar novos serviços não-registrados que por conseqüência poderão surgir, bem como detectar se um processo em execução foi adulterado. Além disso, se um serviço tenta interagir com outras entidades ou com o dispositivo hospedeiro de forma inesperada ou não autorizada, a verificação em tempo de execução deverá detectar e interferir, para evitar uma situação potencialmente perigosa.

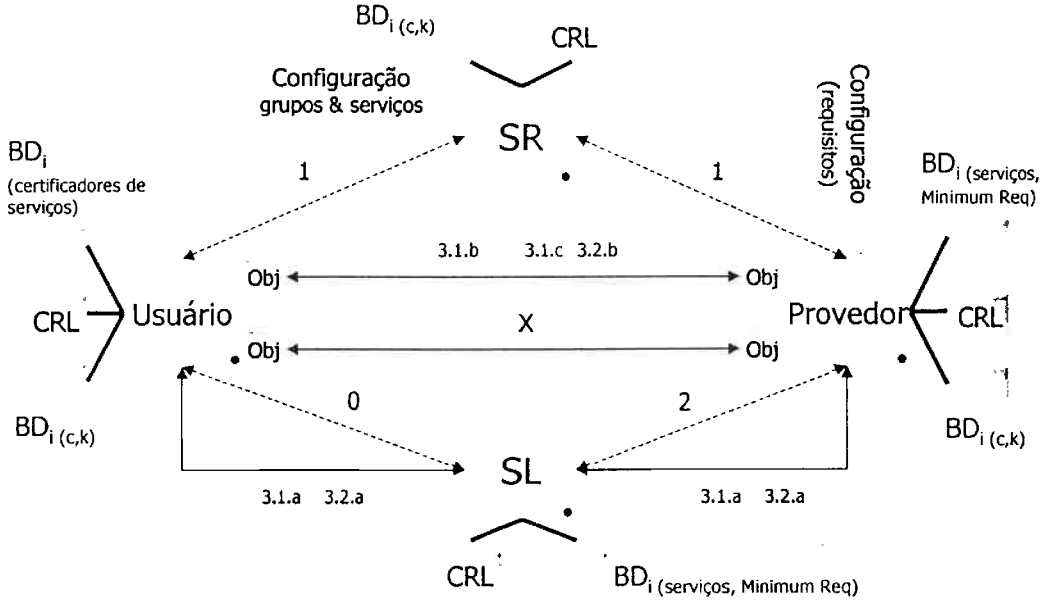
4.7 Considerações

Foram apresentadas as idéias principais relacionadas ao modelo de segurança para redes Ad-Hoc de serviços e foram discutidos alguns dos seus principais aspectos, componentes e mecanismos.

No próximo capítulo descreve-se a arquitetura de segurança que suporta esse modelo.

5 Arquitetura do modelo de segurança para redes Ad-Hoc

A arquitetura do modelo de segurança é composta por um conjunto de entidades e suas respectivas interações. A Figura 5.1 apresenta esquematicamente essa arquitetura e logo a seguir são descritas cada uma das entidades e suas interações e a correspondente base de dados.



Legenda:

SR	Serviço de Registro	SL	Serviço de Localização
$BD_{i(xxx)}$	Base de Dados(conteúdo da base de dados)	CRL	Certificate Revocation List
X	Utilização Direta	Obj	Objeto de Serviço
0	Autenticação de Rede	1	Registro
2	Oferta de Serviço	3.1a	Procura de Serviço
3.1b e 3.1c	Autenticação e Autorização	3.2a e 3.2b	Utilização de Serviços Públicos

Figura 5.1: Arquitetura de Segurança

As linhas tracejadas indicam interações que devem ser feitas previamente à utilização do serviço, enquanto que as linhas cheias indicam interações que devem ocorrer apenas no momento da utilização do serviço.

5.1 As entidades

Este item contém uma descrição sucinta de cada uma das entidades que compõem a Arquitetura de Segurança proposta.

Serviço de Registro (SR) é o responsável pela emissão de certificados de grupo que devem ser aceitos pelas demais entidades, desde que não exista alguma restrição local, como um impedimento explícito a um certificado emitido por um determinado dispositivo. O serviço pode estar hospedado em diversos dispositivos, desde que aptos para tal, ou seja, tenha recursos de processamento e memória compatíveis com as necessidades deste serviço. O Serviço de Registro (SR) também inclui uma lista de revogação de certificados.

Serviço de Localização (SL) é o responsável pela localização dos serviços dentro da rede, além de ser a porta de entrada da rede. Ele é responsável pelo anúncio dos serviços públicos, que não exigem autenticação, e dos serviços privados. Para se ter acesso à lista de serviços privados, o SL exige uma prova de que o dispositivo requisitante de fato pertence à rede. Essa prova é feita através da verificação da posse de uma semente privada, a ser aplicada em um gerador pseudo-aleatório. Um visitante deve utilizar uma semente de visitante para ter acesso aos serviços. Outro ponto importante é que o SL anuncia somente os serviços para o qual o usuário tem direito de utilização. O Serviço de Localização pode estar hospedado em qualquer dispositivo da rede que tenha capacidade para executar tal função, ou seja, tenha recursos de processamento e memória compatíveis com as necessidades deste serviço.

O usuário (U) é a entidade que utiliza o serviço de fato, oferecido pelo provedor (P).

5.2 As interações

As interações seguem uma ordem de execução, numeradas e identificadas na Figura 5.1 referente à Arquitetura de Segurança.

Antes de serem detalhadas as interações, é necessário especificar alguns termos que serão utilizados ao longo do texto, além de algumas trocas de mensagem comuns a várias das interações.

O termo $CERT^{A}_{id}$ é o certificado para a identificação da entidade A frente às demais entidades. Corresponde ao identificador de A (id A), que pode ser o endereço do dispositivo ou o nome do usuário, e a chave pública de A (KU_A) assinada com a chave privada do Serviço de Registro (KPR_{SR}).

$$CERT^{A}_{id} = (id\ A,\ KU_A)KPR_{SR}$$

O termo $CERT^{A}_{grupo}$ corresponde ao certificado de grupo para a utilização de serviços, recebida pela entidade A. Corresponde ao identificador de A (id A) e do nome do grupo ao qual a entidade pertence, assinada com a chave privada do Serviço de Registro (KPR_{SR}).

$$CERT^{A}_{grupo} = (id\ A,\ nome\ do\ grupo)KPR_{SR}$$

A lista de Serviços de Registro, com seus devidos certificados, que podem ser aceitos pelas demais entidades é uma informação sensível e deve estar assinada com a chave privada de um dos dispositivos que hospedam os SR.

$$Lista\ de\ SR = (CERT^{SR1}, CERT^{SR2}, \ldots CERT^{SRn})KPR_{SR}$$

5.2.1 Autenticação Mútua

A seqüência de troca de mensagens conhecida como processo de autenticação mútua é comum a muitas etapas. A Figura 5.2 ilustra este processo.

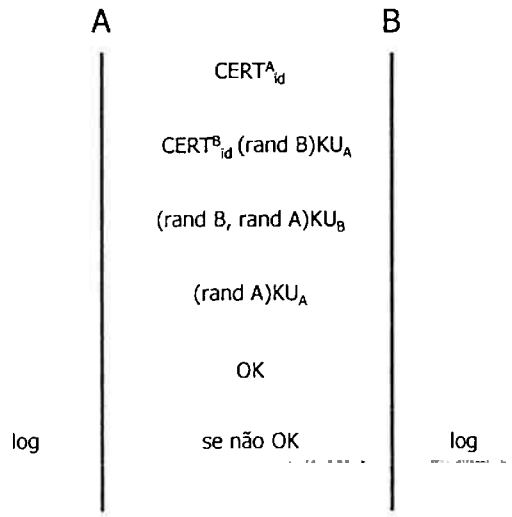


Figura 5.2: Autenticação Mútua

A Autenticação Mútua é um mecanismo necessário para a autenticação das entidades envolvidas. Ela se dá através da troca de certificados, como descrito detalhadamente ao longo deste capítulo.

O processo é iniciado com o envio do certificado de identificação da primeira entidade (A) para a segunda (B). A entidade (B) verifica a autenticidade do certificado enviado por (A) e envia seu certificado para (A) e um número aleatório (rand B), encriptado com a chave pública de (A) (KU_A).

A entidade (A) recebe esta mensagem, verifica a autenticidade do certificado de (B) e extrai o número aleatório (rand B) da mensagem utilizando sua chave privada. A entidade (A) retorna para (B) o número aleatório (rand B) enviado por (B) e um novo número, também gerado aleatoriamente (rand A), ambas encriptadas com a chave pública de (B) (KU_B).

A entidade (B) recupera as informações transmitidas por (A) utilizando sua chave privada. A entidade (B) verifica se o valor (rand B) foi devolvido corretamente. Se correto é enviado para (A) o valor (rand A) encriptado com a chave pública de (A) (KU_A)

Caso todo o procedimento tenha sido executado com sucesso, uma mensagem (OK) é transmitida, finalizando o processo de autenticação mútua.

Caso tenha ocorrido alguma falha no meio deste processo, uma mensagem (NOK), ou seja, não OK, é enviada. Neste caso, *logs* são gerados de forma a permitir eventuais auditorias.

5.2.2 Negociação de Credenciais

A seqüência de troca de mensagens conhecida como processo de negociação de credenciais é também comum a muitas etapas. A Figura 5.3 ilustra este processo.

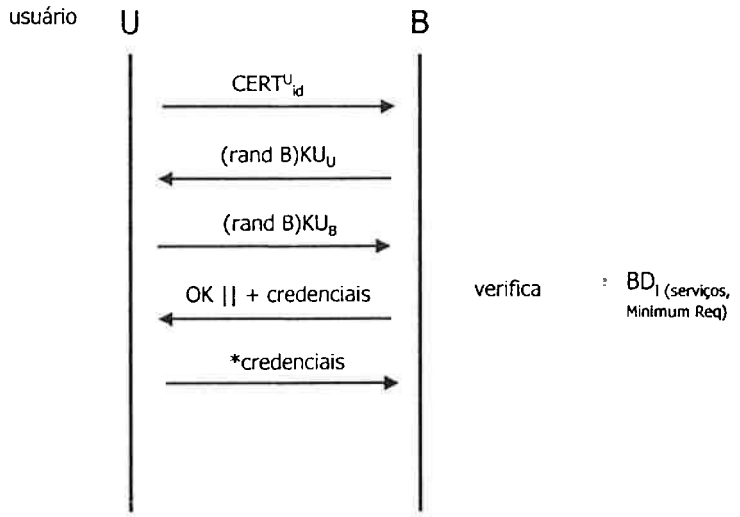


Figura 5.3: Negociação de Credenciais

A negociação de credenciais é necessária para se verificar se o usuário tem direito a utilizar um determinado serviço. Ela é efetuada em duas fases:

Na primeira fase, o usuário (U) envia para o provedor de serviço (como o SL, por exemplo) sua identificação, ou seja, o seu $CERT^{U}_{id}$. O provedor de serviços (B) verifica o certificado e envia para o usuário uma mensagem encriptada (rand B) com a chave pública do usuário (KU_U).

O usuário, através de sua chave privada (KP_U), extrai a mensagem e a devolve para o provedor, devidamente encriptada com a chave pública do servidor (KU_S). O servidor retira a informação útil utilizando sua chave privada (KP_S).

Na segunda fase, o servidor verifica a necessidade de credenciais para o serviço requisitado. Caso não exista a necessidade de credenciais, o provedor retorna uma mensagem OK e executa o serviço. Caso exista a necessidade de apresentação de credenciais, o provedor pede a apresentação das mesmas para o usuário, que transmite uma de suas credenciais. O provedor verifica se a credencial possui os privilégios para que o serviço seja executado. Caso positivo, retorna OK e executa o serviço. Caso negativo, exige novas credenciais. A informação contendo os privilégios necessários para a execução do serviço está armazenada em uma base de dados que relaciona os serviços aos seus requisitos mínimos ($Bd_{i\ (serviços,\ Minimum\ Req)}$).

O processo repete-se até que o usuário apresente uma credencial válida, ou quando o usuário não possui mais credenciais a apresentar, o que acarreta a não utilização do serviço desejado.

Para que uma entidade tenha acesso à rede de serviços, alguns passos devem ser executados. Estes passos estão descritos a seguir:

5.2.3 Passo 0: Autenticação de Rede

O processo de autenticação da rede é o primeiro passo para uma entidade ter acesso à rede de serviços. Toda entidade deve passar, inicialmente, por este processo de modo a ter acesso ou prover serviços à rede. Uma entidade que deseja retornar à rede de serviços deve ser capaz de identificá-la, mesmo tendo passado um grande tempo ausente.

A autenticação de rede consiste de um endereço lógico da rede que deve ser igual a todos os dispositivos pertencentes a esta rede de serviços. Este endereço é dinâmico, ou seja, varia em relação ao tempo, e segue uma seqüência pseudo-aleatória gerada a partir de uma semente.

Esta semente pode ser permanente ou de visitante. Sementes permanentes são seqüências longas de números geradas e trocadas automaticamente pelo sistema, ou seja, o usuário não especifica o seu valor. As sementes de visitante consistem de seqüências menores de números determinadas pelo usuário com um tempo de vida curto. A Figura 5.4 apresenta a troca de mensagens executada no processo de Autenticação de Rede.

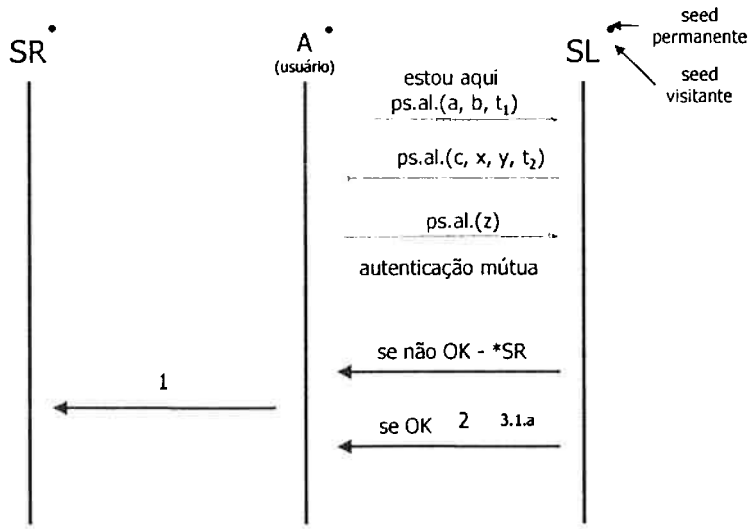


Figura 5.4: Autenticação de Rede

A autenticação de rede é iniciada pelo dispositivo que deseja fazer parte da rede de serviço, seja ele um dispositivo permanente ou visitante. Uma observação importante é que um novo dispositivo permanente deve inicialmente ter uma semente de visitante, de modo a facilitar a entrada do valor da mesma pelo usuário.

O dispositivo (A) deve enviar através de *broadcast* uma mensagem do tipo "estou aqui", tendo como parâmetros dois números consecutivos gerados de modo pseudo-aleatório (a,b) e um eventual terceiro parâmetro temporal (t_1).

O Serviço de Localização (SL) verifica estes parâmetros e determina se estes valores correspondem a uma seqüência esperada, ou seja, se os valores recebidos correspondem aos valores produzidos pelo seu gerador de números pseudo-aleatórios utilizando sua semente, seja ela pública ou privada. Caso negativo, o SL deve não responder e permanecer em silêncio. Caso positivo, deve responder com o terceiro número da seqüência (c), e com dois novos números consecutivos (x,y), também gerados de modo pseudo-aleatório, além de um novo parâmetro temporal (t_2).

O dispositivo deve reconhecer os valores enviados pelo SL e verificá-los. Se o terceiro número (c) corresponder ao valor esperado e a segunda seqüência (x,y) também seja uma seqüência esperada, o usuário responde com o terceiro valor (z). Caso os valores enviados por SL ao dispositivo A não correspondam aos valores esperados, o dispositivo não responde e retorna ao primeiro passo da autenticação.

O SL então verifica se o valor enviado por A corresponde ao valor esperado, e em caso positivo, inicia o processo de autenticação mútua.

Se o processo de autenticação mútua não for efetuado com sucesso, o que pode ocorrer com dispositivos visitantes, ou ainda novos dispositivos, o SL oferece apenas os Serviços de Registro SR disponíveis (passo 1). Se o processo de autenticação mútua ocorrer com sucesso, a oferta de serviços (passo 2) é feita.

5.2.4 Passo 1: O Registro

O registro deve ser previamente configurado pelo administrador do sistema, que estabelece os privilégios de serviços, dispositivos e usuários do sistema, através de uma interface de configuração. O Serviço de Registro (SR) é responsável pela emissão de certificados de identificação e de privilégios para os diversos dispositivos e usuários da rede. Requisitos mínimos para a utilização do serviço também podem ser estabelecidos através do Serviço de Registro, caso não seja possível determiná-los localmente no dispositivo alvo.

O Serviço de Registro pode ser utilizado ainda para a alteração de privilégios das diversas entidades, assim como para a revogação de certificados.

O procedimento de registro é apresentado na Figura 5.5.

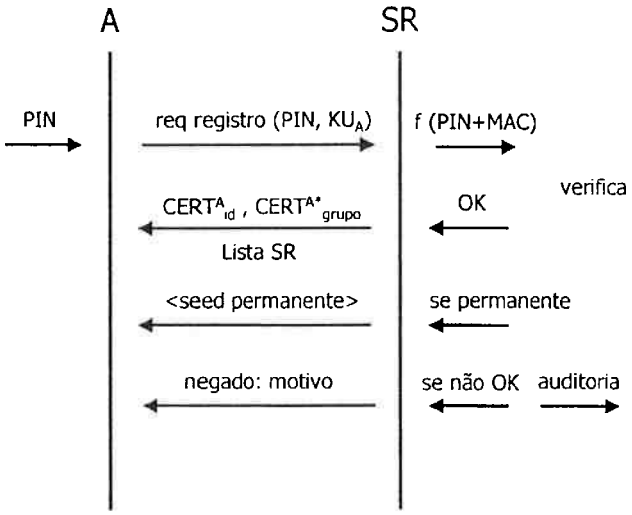


Figura 5.5: O Registro

Para se ter acesso ao Serviço de Registro (SR) é necessário uma senha (PIN), que deve ser enviada pelo dispositivo A, juntamente com sua chave pública (KU_A). A senha (PIN) é de conhecimento do SR e determinada por um usuário privilegiado.

A senha e o endereço do dispositivo são verificados através de uma função (f(PIN+MAC)). Caso a informação esteja correta, ou seja, a senha foi entrada corretamente e o dispositivo reconhecido através de um identificador único, como um endereço de hardware (MAC), esteja realmente sendo esperado na rede de serviços, os seus certificados individual ($CERT^A_{id}$) e de grupos ($CERT^{A^*}_{grupo}$) são transmitidos.

Caso seja um dispositivo novo e que fará parte da rede de serviços como um dispositivo permanente, a semente permanente é transmitida assinada pela chave privada do SR (KPR_{SR}) e encriptada através da chave pública de A (KU_A) para o dispositivo A da seguinte forma.

$$<seed\ permanente> = [(seed\ permanente)KPR_{SR}]KU_A$$

Se a verificação da senha ou do endereço único não for realizada com sucesso, o SR responde com a negação do pedido do registro e o motivo da sua ocorrência. O SR deve também acrescentar estas informações a uma base de dados de forma a ser possível uma eventual auditoria no sistema.

5.2.5 Passo 2: A Oferta de Serviços

A oferta de serviços é realizada por provedores de serviço (B) ao Serviço de Localização da rede (SL). Esta oferta deve passar obrigatoriamente pelos processos de autenticação de rede e de autenticação mútua. O processo de Oferta de Serviços é apresentado na Figura 5.6.

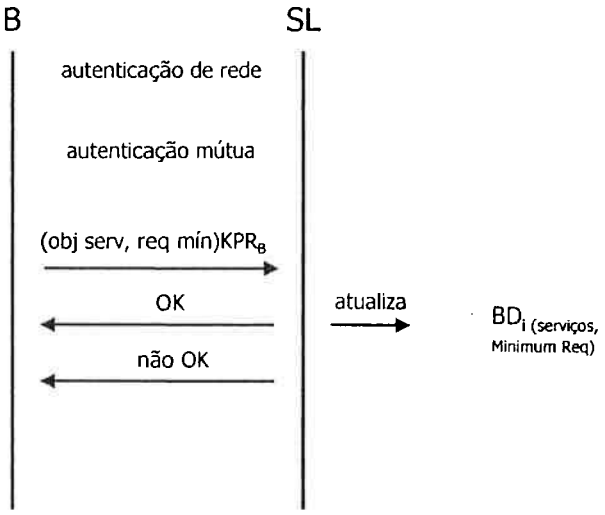


Figura 5.6: A Oferta de Serviços

O provedor de serviços envia uma mensagem assinada com sua chave privada (KPR_S) para o SL contendo o objeto ou a interface de serviço e os seus requisitos mínimos.

O Serviço de Localização atualiza sua base de dados e responde positivamente, caso a atualização tenha ocorrido com sucesso, ou negativamente, caso a atualização da base de dados não tenha sido possível.

5.2.6 Passo 3.2a e 3.2b: Serviços Públicos

Inicialmente é feita a requisição de serviços públicos pelo usuário (A) ao Serviço de Localização (SL). O SL responde com uma lista de zero ou mais interfaces de objeto ou objetos públicos. Como se trata de um serviço público não existe a autenticação entre as partes. O processo de requisição de serviços públicos é apresentado na Figura 5.7.

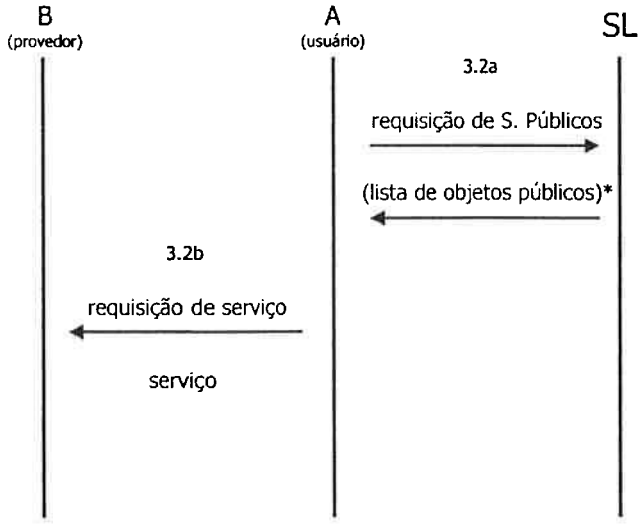


Figura 5.7: Serviços Públicos

A requisição de serviço é feita pelo usuário (A) ao provedor de serviços (B), que realiza o serviço. Novamente, não existe nenhuma autenticação entre as partes.

5.2.7 Passo 3.1a: Procura de Serviço

A procura por um serviço não-público exige que sejam executados os processos de autenticação de rede, de autenticação mútua e caso necessário, o processo de negociação de credenciais. O processo de procura de serviço está ilustrado na Figura 5.8, apresentada abaixo.

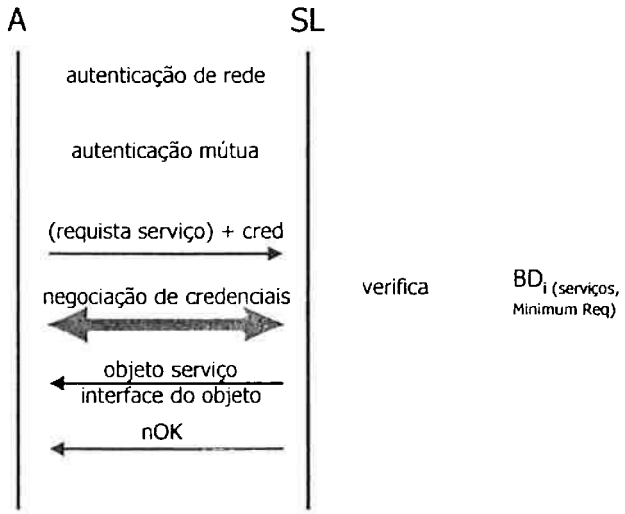


Figura 5.8: Procura de Serviço

Após as fases de autenticação de rede e autenticação mútua serem efetuadas com sucesso, o usuário faz uma requisição de serviço ao Serviço de Localização (SL) acompanhada de zero ou mais credenciais. São verificados a presença do serviço na rede e os requisitos do mesmo e se as credenciais apresentadas são suficientes. Caso o serviço não esteja disponível, o Serviço de Localização (SL) responde com uma mensagem de serviço "inexistente ou indisponível".

Caso o serviço esteja disponível é iniciada a negociação de credenciais para se verificar se o usuário tem direito de receber o serviço.

5.2.8 Passo 3.1b e 3.1c: Autenticação e Autorização

A utilização de um serviço necessita da autenticação mútua entre o provedor de serviço e o usuário, como apresentado na Figura 5.9.

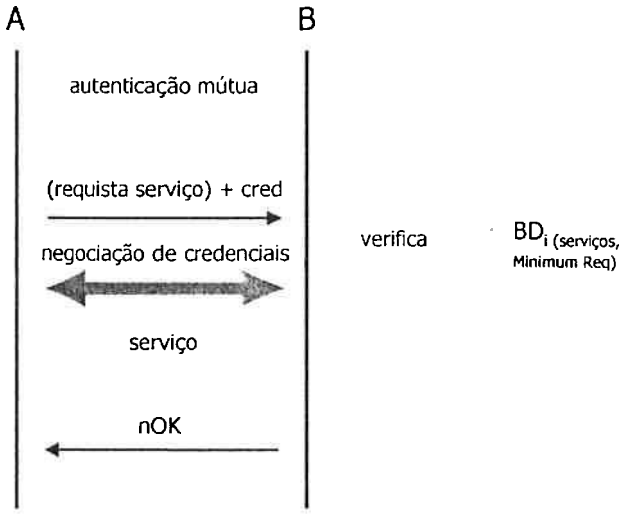


Figura 5.9: Autenticação e Autorização

O processo é praticamente idêntico à requisição de serviço do usuário ao SL apresentado previamente, com exceção da autenticação de rede que não mais é necessária.

5.2.9 Passo X – Utilização Direta

Consiste na utilização direta do serviço pelo usuário. É uma forma de utilização mais rápida do sistema, ideal para a utilização rápida de um serviço, porém menos segura. Pode, também, ser utilizada por dispositivos mais limitados, que não consigam trabalhar com chaves públicas e privadas por limitações de desempenho e capacidade.

Não é utilizado, portanto, o modelo Diffie-Hellman [DIFF76] de criptografia utilizando chaves públicas, mas sim modelos mais leves, como criptografia utilizando chaves simétricas, ou um modelo semelhante ao Kerberos [STEI88], no qual um terceiro dispositivo, como o que hospeda o Serviço de Registro (SR), poderia fazer o papel de servidor de autenticação.

5.3 A base de dados de segurança

As bases de dados consistem de tabelas contendo informações sobre a rede, que devem estar distribuídas nas entidades.

5.3.1 CRL

A CRL (*Certificate Revocation List*) contém a informação relativa aos dispositivos cujos certificados foram revogados. O ato da revogação corresponde a retirar a validade de um certificado não expirado.

Como se trata de uma informação sensível, ela está distribuída entre os diversos dispositivos da rede, que devem ter cópias iguais da mesma tabela (desde que tenham capacidade para tal), já que nem todos SR devem estar obrigatoriamente no

ar o tempo todo. O sincronismo entre as CRL dos diferentes SR, distribuídas entre os dispositivos que compõem a rede, deve ser feito através de um controle de versões individual para cada um dos SR da rede, de modo que as informações contidas nas CRL dos dispositivos da rede seja uniforme.

A atualização das tabelas pode ser feita periodicamente pelos dispositivos, ou através de mensagens enviadas pelo SR (em *broadcast*), que utiliza um controle de versões para o controle das atualizações da lista entre os diversos dispositivos. Uma vez na CRL, uma entidade lá permanece enquanto o seu certificado não tiver expirado ou o SR não tirá-lo da lista, operação que deve ser feito manualmente.

A revogação de um certificado deve obedecer a certas regras e é uma decisão tomada pelo SR a partir de informações sobre o comportamento das diversas entidades participantes na rede.

Caso exista apenas um SR reconhecido no sistema, a operação é simples, o SR revoga o certificado e comunica a operação aos seus pares conforme as regras estabelecidas.

No caso de múltiplas SR presentes no sistema, um certificado pode ser definitivamente revogado após a aprovação de metade dos SR do sistema. Apesar dessa restrição, serviços mais exigentes em relação aos requisitos de segurança, como cofres eletrônicos, podem não aceitar certificados que tenham sido revogados por menos da metade dos SR do sistema.

Caso a CRL atinja um tamanho muito grande, ou seja, comece a afetar o desempenho dos dispositivos da rede de serviço, é possível renovar todos os certificados através da mudança da semente permanente. Este processo pode ser feito automaticamente pelo sistema.

5.3.2 Certificadores de Serviço

Esta base de dados contém uma relação dos certificadores de serviço, ou seja, dos Serviços de Registro (SR) válidos dentro da rede de serviços ao qual o dispositivo faz parte. Estas informações estão contidas em uma lista que é transferida ao dispositivo no momento em que a entidade passa pela fase de registro. Todos os dispositivos da rede devem possuir esta lista.

Esta lista deve estar assinada pelo Serviço de Registro, de modo a garantir a autoria da mesma. O dispositivo verifica de tempos em tempos atualizações nessa tabela, como remoção ou adição de um novo dispositivo a ela.

Políticas de adição ou remoção de Serviços de Registro devem ser adotadas de modo a prover robustez bizantina [KARP00] à arquitetura, ou seja, a rede deve ser capaz de continuar operando mesmo que alguns de seus nós sejam comprometidos, já que Serviços de Registro correspondem aos elementos mais críticos da rede de serviços proposta.

5.3.3 Serviços e Requisitos Mínimos

Esta base de dados contém os serviços oferecidos e os requisitos mínimos necessários para sua utilização.

As entidades provedoras de serviço devem poder exigir zero ou mais requisitos para a utilização de um determinado serviço, como a posse de determinadas credenciais de utilização, ou direitos de acesso somente a alguns usuários cadastrados. Tais exigências podem ser programadas através de uma interface local ou informadas ao dispositivo através da utilização do Serviço de Registro.

O Serviço de Localização (SL) deve apresentar a um requisitante de serviços somente os serviços que ele tem direito de utilizar frente a credenciais apresentadas. Estas exigências são definidas pelo provedor de serviço, que as passa para o Serviço de Localização juntamente com o objeto serviço (ver item 5.2.5). O objeto serviço pode ser um objeto com métodos e atributos próprios para a utilização de um determinado serviço, como uma impressão, por exemplo.

A verificação de credenciais pelo Serviço de Localização (SL) não é a mesma que será efetuada pelo provedor de serviço, mas somente uma verificação inicial, na qual os objetivos seriam apenas determinar se o usuário poderia utilizar um determinado dispositivo ou não.

Podemos afirmar, de modo geral, que a verificação de credenciais feita pelo Serviço de Localização é uma verificação macroscópica de requisitos, enquanto que a verificação executada pelo provedor de serviço contém uma maior quantidade de detalhes necessários para a utilização do serviço fim.

5.3.4 Chaves e Certificados (c,k)

Esta base de dados contém as chaves públicas que o dispositivo conhece, como as chaves públicas dos Serviços de Registro da rede, além da sua própria chave pública. Estas chaves públicas estão relacionadas a dispositivos, que possuem certificados assinados por entidades certificadoras (CA), como visto no diagrama entidade-relacionamento apresentado na Figura 5.10, abaixo:

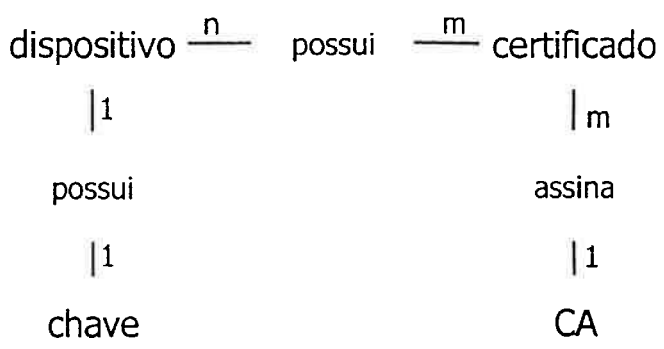


Figura 5.10: Modelo ER da Base de Dados de Certificados e Chaves

A base de dados também contém certificados de utilização de serviços que o dispositivo possui. A chave privada do dispositivo pode estar armazenada nesta base, desde que de modo seguro.

6 Requisitos básicos para aplicações seguras em redes Ad-Hoc: uma verificação de adeqüabilidade

6.1 Aplicação Doméstica - e-Fone

O uso de um serviço de telefone é uma das maiores demandas de uso de serviços domésticos para os usuários. Não somente o serviço de voz regular, mas também a funcionalidade integrada de dados pode tornar essa unidade muito mais usável e conveniente para a comunicação humana e interação com outras pessoas ou com equipamentos e maquinários, em uma configuração local ou remota.

Essa aplicação foi selecionada para ser detalhada neste trabalho para ajudar na identificação dos requerimentos básicos de segurança em um ambiente doméstico e desta forma servir como uma validação informal da adeqüabilidade do modelo de segurança proposto.

O objetivo da estação-base é fornecer serviços de voz e dados para diversas unidades domésticas. A configuração pode ser feita de uma unidade usuária amigável facilitando a interação com o usuário de existência humana. Figura 29 ilustra os elementos básicos que podem ser envolvidos em tais aplicações.

6.1.1 Arquitetura de aplicação

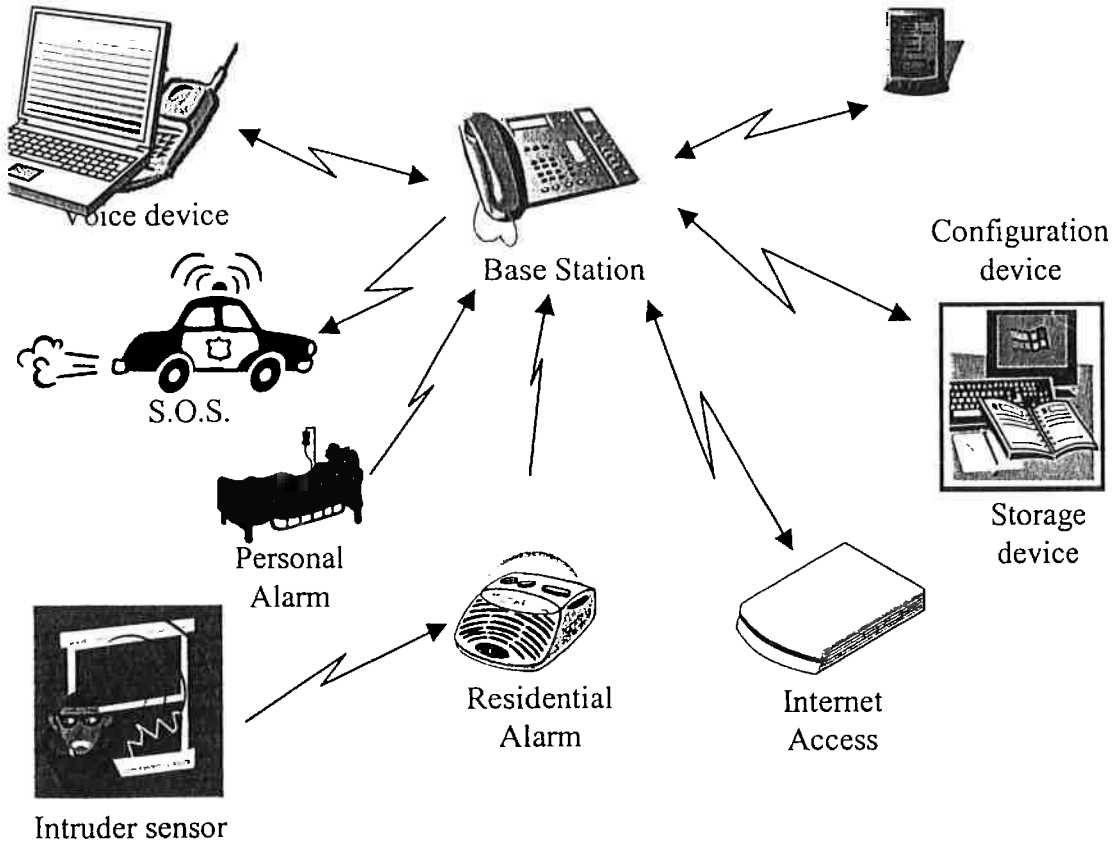


Figura 29: Arquitetura da Aplicação de Telefones

6.1.2 Funcionalidade

6.1.2.1 Dispositivo de voz

A base/central provê acesso a qualquer dispositivo capaz de estabelecer comunicação de voz ou de dados, tal como um telefone celular, telefones de microcomputadores/handsets e computadores com multimídias. O dispositivo de voz pede conexão com a base, que gerencia o uso de canal de voz descarregando ou bloqueando-o, baseado no tipo de chamada solicitada, local, longa distância, ajuda e chamadas a números especiais. Um controle de cota ou de operadoras de telecomunicações pode ser incluído.

O dispositivo de voz pode pedir uso privado do canal de voz para uma chamada. Neste caso, a estação-base comuta para o modo de mono-usuário e bloqueia o canal de voz para outros dispositivos em sua área de alcance.

O dispositivo agindo em modo mono-usuário pode solicitar que outros dispositivos de voz participem do canal de voz. Quando a estação-base recebe a solicitação, altera para o modo multi-usuário, permitindo que outros dispositivos acessem o canal de voz.

Quando uma comunicação entre linhas de ramais é desejada, ela pode ser feita diretamente por dispositivos de voz, sem intervenção da base. O serviço de linha de ramal oferecido pela base só é interessante quando o canal de voz precisa ser transferido a outro dispositivo de voz.

Quando a estação-base recebe um pedido de conexão de voz externa, ela verifica se o número de chamada está registrado como um número especial. Se o número estiver registrado nesta categoria, a base verifica o procedimento associado a este número e o executa. Os procedimentos possíveis são: "Desconectando imediatamente", útil quando alguém está passando trotes freqüentemente e "transmitindo mensagem de voz", útil quando alguém deseja deixar uma mensagem.

Se o número não estiver registrado naquela categoria, a base envia um sinal de chamada a todos os dispositivos de voz registrados. Todos os dispositivos na área de alcance recebem o sinal de chamada e o devolvem. Neste momento, se o dispositivo básico estiver configurado para agir em modo de multi-usuário, todos os dispositivos de voz que fazem parte da conexão de voz acessarão o canal de voz. Porém, se estiver configurado para agir em modo de mono-usuário, só o primeiro dispositivo retornando para a base poderá se conectar e os outros dispositivos serão bloqueados. Uma comutação entre modo mono e multi-usuário pode ser solicitada a qualquer momento.

Se nenhum dispositivo devolver o sinal de chamada enviado pela base, ela passa a agir como secretária eletrônica ou fac-símile.

Outra função da base é prover serviço de leitura de e-mail. O dispositivo de voz solicita à base um serviço de leitura de e-mail que acesse o servidor remoto de e-mail, recuperando mensagens. A base lê o e-mail para o usuário através de reconhecimento de caracteres.

6.1.2.2 Dispositivo de Alarme pessoal e Residencial

O alarme residencial ou pessoal pode requisitar ajuda, enviando o sinal de alarme à base. A base reconhece que dispositivo de alarme está sinalizando, chama o número de telefone pré-configurado pelo respectivo dispositivo e transmite uma gravação de ajuda/socorro.

6.1.2.3 Dispositivo de configuração

A base pode ser configurada a partir de alguns dispositivos amigáveis ao usuário, como desktops, notebooks e equipamentos portáteis, que permitem executar as várias opções de configuração com mais conforto para o usuário.

6.1.2.4 Dispositivo de memória e Dispositivo Conexão com a Internet

A base pode trocar informações sobre registros de telefone com outros dispositivos seja através de consulta ou pela atualização de seu banco de dados . Informações remotas podem ser acessadas através de dispositivos de memória sem fios na rede local ou pelo ponto de acesso à Internet. Este recurso permite consulta às páginas amarelas digitais e à tabela de custo de chamada. Dispositivos de memória podem ser usados para economizar o registro de log e para fazer back-up de usuário ou dados de configuração.

6.1.3 Arquitetura de Serviço

A central telefônica provê serviços de voz para dispositivos de voz e serviços de emergência para dispositivos de alarme, em uma arquitetura cliente/servidor. A central também pode atuar como um cliente para o dispositivo de conexão à Internet. Dispositivos de memória podem ser implementados em uma arquitetura cliente/servidor ou arquitetura peer-to-peer, porque a base e o dispositivo requerem a troca de informações entre si.

6.1.4 Ameaças e Serviços de Segurança

6.1.4.1 Dispositivo de Base e Dispositivo de Voz

Como o dispositivo sem fio extrapola o limite físico da residência, é possível que dispositivos externos tentem utilizar indevidamente a base local para fazer chamadas. A base deve liberar conexão de voz somente a dispositivos autorizados. Para liberar a autorização, os dispositivos de voz devem ser autenticados pela base.

Como o serviço é fornecido tanto para mono como para multi-usuário , a autorização de acesso para canal de voz precisa ser alterada quando uma comutação entre os modos é realizada. O mesmo acontece quando uma chamada é transferida de um dispositivo a outro durante um serviço de linha de ramal.

Outro problema comum é o uso indevido de chamadas de distância longa ou para número especiais. Um controle de acesso deve ser feito para assegurar que somente os usuários autorizados façam tais chamadas . Os usuários precisam ser autenticados. Isto pode ser feito por reconhecimento de voz, senha ou outra autenticação disponível.

Adicionalmente, pode ser feito um controle de acesso por quotas ou operadora de telecomunicação. Isto evita problemas com o custo de uso de sistema.

Em ambientes sem fio, qualquer um pode receber o sinal de comunicação. Esta é uma ameaça à privacidade do usuário quando a comunicação de voz for secreta. Serviços de confidencialidade devem ser adicionados ao serviço de voz.

Finalmente, para facilitar a detecção de falhas e ameaça à segurança, todas as falhas de acesso devem ser registradas. Um serviço de registro de ocorrências deve ser incluído.

6.1.4.2 Dispositivo de Alarme Pessoal e Residencial

Este tipo de serviço pode ser ameaçado por um falso dispositivo de alarme que requisita um serviço de emergência para a estação-base. Os dispositivos de alarme devem ser autenticados antes de utilizarem o serviço de emergência para evitar este tipo de ataque.

Quando um dispositivo válido solicita um serviço de emergência e a estação-base não o recebe, um ataque de interrupção pode estar acontecendo. Uma solução para se evitar este tipo de problema pode ser a transmissão periódica de sinais "keep alive" do alarme para a estação-base. Se o sinal "keep alive" não for recebido depois de um período de tempo estabelecido, um número de telefone configurado deve ser chamado ou um alarme, ativado.

Todas as rupturas, falhas ou ameaças do sistema de segurança devem ser registradas em log a fim de se manter um registro cronológico para gerenciamento de segurança.

6.1.4.3 Dispositivo de configuração

Um ataque ao dispositivo de configuração pode ser feito a partir de um acesso de dados impróprio, um uso de linha telefônica sem autorização ou até mesmo um serviço de emergência não concluído. Devido a todos esses fatores, dispositivos e usuários devem ser autenticados e autorizados para terem acesso a estes serviços.

A integridade da configuração de dados deve ser garantida a fim de prevenir um ataque de modificação. Quando os dados secretos são enviados, como documentos confidenciais, ou armazenados, como senhas ou chaves de segredo/secretas, tem que existir um serviço de confidencialidade.

Todo o serviço de configuração deve ser registrado para evitar um ataque de não repudiação.

6.1.4.4 Dispositivo de memória e Dispositivo de Conexão à Internet

As exigências de segurança para troca de dados entre a estação-base e o dispositivo de memória são dependentes do próprio serviço específico. Mas todos os dispositivos que trocam dados devem ser autenticados e autorizados.

A estação-base, ao prover ou atualizar dados a outro dispositivo, requisita um serviço de integridade, para garantir a correta entrega de dados, e um serviço de confidencialidade, se os dados forem secretos. Mas se outro dispositivo requisita uma atualização de dados à estação-base, os serviços de autenticação de

integridade, confidencialidade e autenticação de usuário são necessários porque é possível ocorrer um ataque de modificação.

O back-up ou registro em log de dados armazenados em um dispositivo remoto estão suscetíveis às mesmas ameaças de segurança daquele dispositivo. Desta forma, o dispositivo remoto precisa ser confiável e precisa ter capacidade de memória/armazenamento de segurança. A autenticação mútua é necessária entre a estação-base e o dispositivo de memória a fim de permitir um serviço de memória de segurança. A autenticação de usuário também é necessária para liberar acesso escrito a dados.

6.1.5 Serviço de segurança

A Tabela 7 apresenta os serviços que necessitam ser implementados a fim de se garantir segurança à funcionalidade de cada base.

Security / Function	Authentic. Device	Authorization				Access Control				Integrity	Confidentiality		Log
		Voice Channel	Emergency	User data	Config. Data	User Authent.	Types of Call	Quote	Telco		Data	Voice	Register
Emergency	X→	X	X				X						X
Fax/Voice local	←X→	X					X					X*	
Fax/Voice spec	←X→	X				X	X	X	X			X*	X
Switching		X											
Extension Line	X→	X											
Data-query	←X→			X						X*	X*		
Data-download	←X→			X						X*	X*		
Data-upload	X→			X		X				X*	X*		X
Config.	←X→				X	X				X	X		X
Receive call	←X→	X					X						X
Access Info	←X→	X		X		←X							X
Store Info	←X→			X	X	X				X	X*		X
	←X→												

Tabela 7: Serviço de segurança x Funcionalidade

→ Base authenticate device
← Device authenticate base
* Optional

6.1.6 Exemplos de Uso do Módulo de Segurança na Aplicação Telefônica

6.1.6.1 Serviços de voz

Como estabelecido nos requisitos de segurança do aplicativo, antes que qualquer serviço de voz possa ser utilizado, o dispositivo deve ser identificado e autenticado. Desta forma, um registro de dispositivo de voz é necessário, e, para qualquer serviço de voz, a identificação de usuário e autenticação são necessárias. Neste caso, o usuário precisa ser registrado.

Como exemplo, considerar os dispositivos e usuários registrados apresentados nas Tabela 8 and Tabela 9, respectivamente.

Tabela 8: Lista de Dispositivos para Aplicação em Telefone

Lista de Dispositivos
Celular 1
Celular 2
Telefone de microcomputador 1
Computador 1
Central
Alarme 1 – Residencial
Alarme 2 – Pessoal
Sensor 1
Sensor 2
Sensor 3

Tabela 9: Lista de Usuários para Aplicação em Telefone

Lista de Usuários
Mãe
Pai
Filho1
Filho 2
Funcionário 1
Funcionário 2

Antes que um usuário ou dispositivo registrado possa usar o serviço de voz, eles devem ser identificados e, por conseguinte, devem ser autorizados para este uso específico.

A base para esta autorização é a atribuição de direitos de acesso fornecida no modelo de segurança. Um exemplo das ações permitidas para o serviço de voz está

apresentado na Tabela 10. Pode-se notar que o serviço precisa de diferentes níveis de controle nas operações.

Tabela 10: Lista de ações para o serviço de voz

AÇÃO	DESCRIÇÃO
Chamada de Voz Local	Acesso a canal de voz para fazer uma chamada local
Chamada de Voz de Longa Distância	Acesso a canal de voz para fazer uma chamada de longa distância
Chamada de Voz Especial	Acesso a canal de voz para fazer uma chamada para um prefixo especial
Internet	Acesso ao canal de voz para uma conexão com a Internet
Transferência de Voz	Para transferir um canal de voz para outro canal
Modo de Voz	Para alternar entre modo mono e multi-usuário durante uma conexão de voz
Recepção de Chamada Voz	Receber chamada para canal de voz

Como no modelo de segurança, os usuários estão classificados em grupos, que estão associados a perfis.

Tabela 11 mostra o mapeamento de alguns grupos para os usuários e dispositivos apresentados na Tabela 9 e Tabela 8. Tabela 12 mostra o mapeamento de grupos aos perfis.

Tabela 11: Mapeamento de Grupos X Entidades para a Phone Application

Grupo	Entidade
Pais	Mãe, Pai
Filhos	Filho 1, Filho 2
Funcionários	Funcionário 1, Funcionário 2
Voz	Celular 1, Celular 2, Telef. de PC, Computador 1
Residencial	Alarme 1
Pessoal	Alarme 2
Alarme 1 SENS	Sensor 1, Sensor 2
Alarme 2 SENS	Sensor 3

Tabela 12: Mapeamento de Perfis X Grupos para a Phone Application

Perfil	Grupo
Administrador	Pais
Moradores	Pais, Filhos

Funcionários	Funcionários
Privilegiados	Pais
Voz	Voz
Alarmes	Residencial, Pessoal,
Sensores RES	Alarme 1 SENS, Alarme 2 SENS, Residencial, Pessoal

Finalmente, permissões de ações estão associadas a perfis, permitindo o controle de acesso das ações. Tabela 13 mostra um exemplo desta associação para o serviço de voz.

Tabela 13: Perfis para o serviço de voz em Phone Application

	Perfis				
Ações	**Administrador**	**Moradores**	**Funcionários**	**Privilegiados**	**Voz**
Chamada de Voz Local		X	X		X
Chamada de Voz de Longa Distância		X			X
Chamada de Voz Especial				X	X
Internet		X			X
Transferência de Voz		X			X
Modo de Voz		X			X
Recepção de Chamada Voz		X	X		X

6.1.6.2 Central e Dispositivo de Alarme (Residencial e Pessoal)

Como os dispositivos de alarme não estão associados aos usuários, então não são capazes de identificá-los. Apenas a identificação de dispositivo é usada no processo de autenticação. A Tabela 14 e

Tabela 15 apresentam a lista de ações e perfis relacionados aos serviços de alarme que foram incluídos na Tabela 11 e Tabela 12 para controle de acesso no serviço de alarme.

Os alarmes são ativados através de sensores externos ou manualmente. Quando o dispositivo de alarme estiver ativado, eles podem solicitar à central para discar um número de emergência específico.

Tabela 14: Lista de Ações

AÇÃO	DESCRIÇÃO
Alarme 1 DISP	Ative um alarme
Alarme 2 DISP	Ative um alarme
Solicitação de Ajuda	Ative o serviço de chamada de emergência na central

Tabela 15: Perfis para a Phone Application

	Perfis		
Ações	**Alarmes**	**Sensores RES**	**Sensores PES**
Alarme 1 DISP		X	
Alarme 2 DISP			X
Solicitação de socorro	X		

6.1.6.3 Central e Dispositivo de Configuração

O serviço de configuração somente está liberado no perfil do administrador. A necessidade de mecanismos de integridade é o principal diferencial deste serviço. Alguns dados secretos podem ser armazenados, como senhas de usuários, implicando no uso de mecanismos de confidencialidade especificados pelo modelo de segurança.

O serviço de configuração deve usar um serviço de registro para permitir verificação de pós-operação. O modelo de segurança especificado permite este tipo de controle através do mapeamento do serviço de grupo de entidade para um perfil autorizado a usar o serviço de registro. Neste caso, o serviço deve poder identificar a si próprio e ser autenticado.

6.1.6.4 Central, Dispositivo de Memória e Conexão á Internet

Este serviço requer autenticação mútua, mecanismos de integridade e confidencialidade, necessários para proteger dados transmitidos e armazenados. Necessita de registro histórico de todos os processos de memória.

6.1.7 Assinaturas digitais

Uma assinatura digital é um método adotado entre entidades (pessoas ou dispositivos) usada para autenticar de uma maneira sem igual a identidade destas entidades ou as informações produzida por elas.

As assinaturas digitais são geradas pelas entidades de uma maneira que deveria ser única a todas elas, normalmente baseadas em suas características individuais. Nossas impressões digitais são únicas e nossas assinaturas manuscritas podem ser relacionadas a nós de um modo semelhante.

A assinatura digital é usada para dois fins principais:

- Autenticação (provar identidade)
- Não-repúdio (provar autoria)

6.1.7.1 Classificação

As assinaturas digitais podem ser divididas em duas categorias principais: biométricas e baseadas em chaves.

6.1.7.1.1 Assinaturas Biométricas

As assinaturas biométricas estão baseadas em características físicas de cada entidade que podem ser capturadas e convertidas em dados digitais. Exemplos típicos são impressões digitais, escaneamento de retina , face, voz e assinatura manuscrita.

As assinaturas biométricas somente são usadas para a identificação de uma entidade, ou seja, para provar que alguém é realmente quem reivindica ser.

6.1.7.1.2 Assinaturas baseadas em chaves

As assinaturas baseadas em chaves usam uma infra-estrutura de chave pública (PKI, Public Key Infrastructure). Cada usuário desta infra-estrutura gera uma dupla de chaves. Uma destas chaves é mantida em segredo pelo usuário e é chamada "Chave Privada." A outra chave é chamada "Chave Pública" e é enviada a uma entidade certificada chamada Autoridade Certificadora (CA, Certification Authority). Estas chaves têm a propriedade que uma mensagem criptografada com uma deles só pode ser decriptografada com a outra.

Portanto, se alguém quiser enviar uma mensagem criptografada a um receptor, pedirá o Certificado de receptores para a CA. O certificado é um documento eletrônico que contém algumas informações sobre o receptor e sua chave pública. O remetente leva a mensagem, a codifica com a chave pública do receptor e a envia.

Somente o receptor tem a habilidade para decifrar a mensagem, uma vez que mensagens criptografadas com uma chave pública somente podem ser decifradas pela chave privada correspondente.

O contrário também é válido e usado para produzir assinaturas baseadas em chave digital.

Se alguém quiser verificar a autoria de uma mensagem, solicitará que o remetente a assine digitalmente. Isto é feito criptografando-se a mensagem inteira ou seu hash com a chave privada do remetente. O receptor pode então decifrar a mensagem (ou hash) com a chave pública do remetente e verificar o resultado: uma mensagem legível ou hash corretoAplicações exemplo e cenários de uso

6.2 Considerações sobre a adeqüabilidade do modelo de segurança proposto

Através de um exercício sobre a aplicação dos conceitos envolvidos no modelo de segurança proposto a um serviço, típico de uma rede Ad-Hoc doméstica o serviço de

voz - e-phone, pode-se verificar a adeqüabilidade do modelo para suportar as questões de segurança neste tipo de aplicação.

De uma forma mais importante, deve-se observar que os aspectos mais inovadores do modelo dizem respeito ao tratamento das características dinâmicas das redes Ad-Hoc e do processo de distribuição de confiança nesse ambiente.

Acredita-se que desta forma, o modelo proposto representa uma evolução muito importante em relação ao modelo de segurança Java incorporando o tratamento da variação temporal nas relações de confiança, através da aplicação de uma máquina de estado finito que captura as possíveis trajetórias de mudanças de estado relativas aos usuários permanentes e temporários deste sistema.

A possibilidade de se mensurar a relação de confiança baseado em informações cadastrais, comportamentais, credenciais ou biométricas obtidas durante um processo de autenticação, representa um passo fundamental para tratar as incertezas associadas a este ambiente. A natureza probabilística de tal medida permite lidar de uma forma adequada com a incerteza inerente a esta avaliação.

Finalmente, o processo de distribuição de confiança permite eliminar, definitivamente, a necessidade de uma unidade central única para se garantir as decisões nos processos críticos de segurança.

Um passo fundamental para a consolidação do modelo definido é a sua implementação com o intuito de se constatar não só que ele representa um conjunto de funcionalidades suficientes para os ambientes de redes Ad-Hoc como também, é perfeitamente possível de se obter uma implementação eficiente, mesmo em dispositivos simples. Diversos trabalhos de mestrado e doutorado orientados pelo autor estão sendo conduzidos nessa direção.

7 Conclusões e trabalhos relacionados

Através de um processo de análise e pesquisa foi identificado neste trabalho a necessidade de se reformular certos conceitos, tradicionalmente utilizados nos modelos de segurança atualmente disponíveis, para tratar este aspecto tão sensível dos sistemas de informação on-line, principalmente aqueles que se interconectam de alguma forma a Internet.

As redes Ad-Hoc tem surgido como uma alternativa natural para diversas situações comumente encontradas em nosso dia-a-dia. A facilidade de se implantar tais redes pelo fato delas não necessitarem de nenhuma infra-estrutura pré-estabelecida, torna este tipo de arquitetura muito atraente para situações que apresentam características dinâmicas associadas aos seus usuários. Nestes ambientes existe também incertezas que dificultam sobremaneira as decisões que envolvem os aspectos de segurança da informação ou da comunicação.

Dentre os modelos de segurança disponíveis, destaca-se o da linguagem Java. Este modelo experimentou uma evolução significativa nos últimos anos tendo sido incorporado a ele inúmeros conceitos novos e técnicas robustas de segurança que representam um enorme avanço no tratamento das questões de segurança em redes de computadores.

Apesar desta evolução acentuada, o modelo Java não trata adequadamente as questões relativas as variações temporais, naturalmente existentes nas redes Ad-Hoc. As relações de confiança são tratadas de maneira estática ou muito lentamente variáveis tornando-se difícil a aplicação desse modelo para os ambientes dinâmicos inerentes as redes não estruturadas sem fio.

O dinamismo presente nas redes Ad-Hoc se caracteriza por variações temporais em diversas dimensões . Ora é o estado de um usuário que pode variar entre diversas categorias dentro da classe de temporários, ora são as permissões de acesso a serviços da rede, ora é a ausência ou o retorno de serviços normalmente existentes na rede, ora são usuários que saem ou entram no raio de alcance da redes sem fio, ora são as relações de confiança que se alteram devido a processos de autenticação ou devido ao comportamento operacional de usuários, serviços ou dispositivos, enfim, existe uma gama muito grande de variabilidades nesses ambientes que não são adequadamente tratadas pelos modelos de segurança presentemente disponíveis.

Com o intuito de equacionar esse conjunto de demandas provocadas pelo dinamismo dos ambientes Ad-Hoc, este trabalho propõe um novo modelo de segurança e confiança, em alguns aspectos derivado do modelo Java, porém que incorpora conceitos e técnicas novas e adequadas ao tratamento eficaz da variabilidade de certas grandezas e características dos sistemas de informação seguros que devem ser implantados sobre redes de comunicação sem fio.

No desenrolar dos trabalhos uma série de requisitos foram identificados e que deveriam estar presentes no novo modelo. Tais requisitos são aqui reproduzidos com o intuito de identificar essas características e também comentar e mostrar como o modelo proposto trata essas questões ou resolve os correspondentes problemas:

- ***A hierarquia de confiança não deve depender exclusivamente de um único nó central;***
    - O modelo proposto não depende necessariamente de uma única autoridade certificadora responsável pela emissão de certificados digitais que são utilizados nos processo de autenticação e utilização de serviços. Estes certificados também são empregados no processo de atribuição e distribuição de confiança. Em princípio, todos os nós responsáveis pelo provimento de serviços podem emitir os seus certificados, para uso local ou para uso mais abrangente em função das relações de confiança por eles mantidas.. Apesar dessa característica de controle distribuído, o modelo pode facilmente conviver, temporariamente, com a presença de uma autoridade única no raio de alcance da rede.
- ***O modelo deve apresentar solução de proteção para todos componentes inteligentes (com capacidade de processamento) da rede, pois não existirá um único ponto de entrada nessa rede;***
    - Nas redes tradicionais pode-se limitar os pontos de entrada numa dada rede. Nas redes Ad-Hoc, em princípio, todos os dispositivos participantes do ambiente estão sujeitos a receber elementos intrusos que eventualmente possam querer participar indevidamente das transações em curso na rede. O modelo proposto se baseia nos mesmo princípios do modelo Java, restringindo as ações que um programa remoto possa ter em qualquer dispositivo pertencente a rede Ad-Hoc. A utilização de assinaturas digitais com verificações antes e durante a execução dos programas garante que mesmo os dificílimos e indesejáveis vírus possam ser evitados.
- ***O conceito de confiança deve ser criado ou estabelecido a partir de condições iniciais ("set-up") e pode ser alterado/aprimorado dinamicamente baseado no comportamento dos nós da rede durante a operação da mesma;***
    - Este é uma das maiores contribuições apresentadas pelo modelo proposto. Foi definido uma forma de se tratar e mensurar a confiança, que pode inclusive variar no tempo. Através de um rico conjunto de mecanismos de autenticação pode-se atribuir inicialmente uma medida da confiança de um nó em relação a outro. Neste processo de autenticação são utilizadas informações secretas (senhas, sementes, etc.), informações cadastrais e comportamentais além de credenciais ou recomendações que podem ser utilizadas em conjunto com características biométricas. Este conjunto rico de informações permite designar uma medida inicial de confiança. Essa medida é expressa por uma dupla que indica o grau de confiança e o grau de desconfiança existente na relação. Essa medida é utilizada para se estabelecer a mínima confiança necessária ou a máxima desconfiança tolerável para se ter acesso a um recurso ou serviço da rede. Com o desenrolar da operação da rede, as entidades vão apresentando um comportamento operacional que vem enriquecer enormemente estas informações permitindo que as medidas de confiança/desconfiança possam variar

refletindo a situação dinâmica do usuário na rede. Adicionalmente, o modelo consegue tratar a questão da distribuição da confiança, definindo um mecanismo para a transferência transitiva da mesma entre diversos nós da rede. Esta cadeia de transferência também representa um outro ponto de modelagem da variabilidade e das incertezas naturais das redes Ad-Hoc.

- ***Deve-se definir uma maneira pragmática de se avaliar as relações de confiança baseado num processo inicial de autenticação;***
    - O processo de avaliação da confiança se materializa no mecanismo de autenticação e pode utilizar informações de natureza secreta, cadastrais, comportamentais, credenciais ou biométricas. O modelo prevê que com a utilização dessas informações possa-se definir uma tabela para cada entidade que expressa a relação de confiança/desconfiança dela com os outros elementos da rede. Na prática, pode se aplicar esse mecanismo baseado em informações iniciais cadastrais e credenciais e com o passar do tempo, baseado em informações comportamentais, esse valor vai sendo modificado de forma a sempre representar a estimativa atual da medida de confiança nas relações entre os nós da rede.
- ***O modelo deve prover mecanismos de autenticação mútua entre nós usuários e nós provedores de serviços;***
    - Esta necessidade é facilmente atendida pelo modelo pois os protocolos de segurança típicos possuem mecanismos de desafio-resposta que podem ser utilizados em parcerias com criptografia de chaves públicas para se garantir, sempre que necessário, as autenticações mútuas.
- ***O modelo deve se basear, na medida do possível, no modelo de segurança Java versão 2, para manter compatibilidade ou mesmo poder utilizar os resultados positivos já alcançados e que forem aplicáveis ao ambiente de redes Ad-Hoc;***
    - O objetivo deste requisito é o de tornar fácil a migração de aplicações já existentes no ambiente Java para este ambiente de redes móveis. As características de filtragem, "sandbox" e granularidade seletiva na atribuição de permissões evidenciam que o modelo proposto incorpora todas as característica relevantes ao modelo proposto e existentes no modelo de segurança Java versão2;
- ***O modelo deve tratar adequadamente os visitantes desejados e implacavelmente os intrusos, procurando definir um compromisso equilibrado entre flexibilidade de utilização e segurança;***
    - Nos ambientes de redes Ad-Hoc, convivem tanto os visitantes desconhecidos, porém bastante desejáveis, pois eles podem participar de transações, inclusive comerciais, com intrusos indesejáveis, que procuram sempre tirar proveito de alguma falha na proteção dos sistemas de informação. O modelo proposto, através da característica de obtenção gradual de confiança permite que os visitantes desejáveis que se comportam exemplarmente, possam ir crescendo a medida de

confiança e decrescendo a de desconfiança que os serviços da rede atribuem a eles. Já os intrusos indesejáveis, passam por processo inverso, pois a cada atitude inadequada, a medida de confiança ou de desconfiança que os serviços da rede atribuem a ele decresce ou cresce respectivamente, de maneira bastante rápida, tornando o sistema implacável com este tipo de elemento.

- ***O modelo deve captar e poder lidar adequadamente com a natureza dinâmica, móvel e mutante dos nós das redes Ad-Hoc, reagindo coerentemente nas situações inusitadas naturalmente provocadas por esse dinamismo;***
    - A descrição do requisito anterior demonstra essa propriedade do modelo proposto. Esta capacidade é demonstrada pelo modelo ao reagir com um aumento gradual da confiança depositada num visitante desejado e com um decréscimo abrupto na desconfiança atribuída a um intruso. O próprio mecanismo de distribuição transitiva de confiança ajuda a ilustrar também este aspecto tão importante do modelo.
- **O modelo de segurança deve focalizar preferencialmente o conceito de prestação de serviços (redes de serviços) pois é através desse conceito que se atinge ou se atende as necessidades dos nós usuários das redes Ad-Hoc;**
    - A estrutura de permissões dos provedores de serviço da rede garante esta característica. Os serviços são os elementos fundamentais do sistema. Sem eles nada de útil é realizado. Por isso, eles tem condições de atuar na sua própria proteção baseado no nível de permissões existentes e na medida de confiança atribuída a cada instante, a todas as entidades da rede. A existência do serviço de localização e do de registro permite aliviar os prestadores de serviços das tarefas custosas de gerenciamento de bases de dados de permissões e credenciais, libertando capacidade de processamento para ser utilizada na prestação direta de serviços e na sua correspondente qualidade.
- ***O modelo não deve impedir a participação de dispositivos simples e não inteligentes, com um nível de segurança compatível com suas capacidades e sem comprometer a segurança da rede como um todo;***
    - A flexibilidade é um atributo importante e sempre existente no modelo proposto. Ele permite a convivência de procedimentos ou mecanismos sofisticados com outros bastante simples, de forma que os dispositivos possam se adaptar as suas necessidades ou capacidades procurando atingir um compromisso adequado entre a segurança, a flexibilidade e o desempenho.
- ***As relações de confiança devem poder ser aplicáveis em diversos níveis de granularidade e de forma totalmente seletiva para compatibilizar a natureza diversa e dinâmica dos nós participantes das redes Ad-Hoc.***
    - As permissões tratadas pelo modelo podem ser definidas em diversos níveis de granularidade. Pode-se permitir ou negar o uso completo de

serviços ou simplesmente de parte das funções disponibilizadas por eles. Esta decisão é específica e cabe ao administrador do serviço exerce-la. O modelo não impõe nenhuma limitação nesse aspecto oferecendo total flexibilidade e granularidade no tocante a proteção ou permissões de serviços nas redes Ad-Hoc.

Um aspecto muito importante que deve ainda ser verificado, através da execução de diversos trabalhos de mestrado ou de doutorado, que estão em andamento sob a orientação do autor, diz respeito a implementação do modelo de segurança proposto. Estas implementações estão sendo desenvolvidas de forma a constituir um laboratório de teste para o desenvolvimento de aplicações seguras para redes Ad-Hoc. Este ambiente de desenvolvimento e teste deve permitir também que aspectos ligados diretamente as tecnologias básicas utilizadas possam ser exercitados e investigados. Desta forma, se materializa a intenção de se implantar um ambiente razoavelmente genérico para a experimentação e o desenvolvimento de redes Ad-Hoc e sua aplicações seguras.

Os resultados e contribuições conseguidas com este trabalho vem se somar a outras importantes inovações que foram obtidas nos últimos anos, pelas equipes do LARC e da Scopus Tecnologia sob orientação e coordenação do autor.

8 Referências Bibliográficas

Diversas publicações foram consultadas mas não aparecem referenciadas no texto, porem, certamente elas se constituem num acervo importante para o posicionamento da área. Tais publicações estão referenciadas em relatórios técnicos do LARC onde elas são pertinentes. A lista de referências logo abaixo contem somente aquelas publicações diretamente mencionadas e relevantes a este trabalho.

[802.11] IEEE Std 802.11 - **Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) specifications**, 1999.

[802.11A] IEEE Std 802.11a - **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band**, 1999.

[802.11B] IEEE Std 802.11b - **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band**, 1999

[BALL01] Ballai, P.; Singh G. – **Wireless LANs: Look at Issues and Actions for Effective Deployment, Maximum Performance and Efficient Maintenance** – Networld+Interop, Las Vegas – NV, EUA, 2001.

[BLUE01A] Bluetooth SIG – **Specification of the Bluetooth – Core, version 1.1** – specification volume 1, February 2001.

[BLUE01B] Bluetooth SIG – **Specification of the Bluetooth – Profiles, version 1.1** – specification volume 1, February 2001.

[BRAY00] Bray, J.; Sturman, C.F. – **Bluetooth: Connect without Cables** – Prentice Hall, 2000

[CABR99] Cabral Jr, E.F. - **Notas de Aula do Curso de Engenharia de Comunicações**. - Departamento de Engenharia Eletrônica. Universidade de São Paulo, 1999.

[CALO00] Câmara, D.; Loureiro, A. A. F. **Redes de Computação Móvel Ad-Hoc**. http://www.siam.dcc.ufmg.br/gedoc/, 2000.

[DILL89] Dillard, R.A.; Dillard G.M. – **Detectability of Spread-Spectrum Signals** – Artech House, 1989.

[FRJO00] Frodigh, M.; Johansson, P.; Larsson, P. - **Wireless ad hoc networking – The art of networking without a network** - Ericsson Review No. 4, 2000.

[GARF96] Garfinkel, S., Spafford, G. - **Practical Unix and Internet Security**. 2nd Edition, O´Reilly and Associates, 1996.

[GINS84] Ginsgerg, M. - **Non-Monotonic reasoning using Dempster´s rule**, Proc. Of the AAAI-84, Austin, TX. Pp. 125-129, 1984.

[HELD00] Held, G. - **Data Over Wireless Networks: Bluetooth, WAP & Wireless LANs** – McGraw Hill, 2000.

[HERM99] Hermelin, M. Nyberg, K. (Nokia Research Center, Helsinki, Finland) - **Correlation Properties of the Bluetooth Combiner** – 1999.

[HOWA97] Howard, John - **An analysis of secure incidents on the internet**. PhD dissertation, Carnegie Mellon University, 1997

[JESZ91] Jeszensky, P.J. E. **Notas de Aula do Curso de Comunicação por Espalhamento Espectral**. Departamento de Engenharia Eletrônica, Universidade de São Paulo, 1991.

[JESZ92] Jeszensky, P.J.E. – **Notas de Aula do Curso de Comunicação por Espalhamento Espectral: Uma motivação para o estudo de seqüências de código** – Departamento de Engenharia Eletrônica, Universidade de São Paulo, 1991.

[KÄRP00] Kärpijoki, V. - **Signalling and Routing Security in Mobile and Ad-hoc Networks** - http://hut.fi/~vkarpijo/iwork00/, 2000.

[MARU01] Matayoshi, C. M., Ruggiero, W. V. **Modelo de Segurança da Linguagem Java - Problemas e Soluções**. Universidade de São Paulo, 2001

[MDOY98] Macgregor, R.; Durbin, D., Owlett, J., Yeomans, A. - **Java Network Security**. Prentice Hall, 1998.

[MILL99] Miller, B.A.; Bisdikian, C. – **Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications** – Prentice Hall, 2000.

[MULL00] Muller, N.J. – **Bluetooth Demystified** – McGraw Hill TELECOM, 2000

[MULL99] Muller, T. - **"WHITE PAPER: Bluetooth Security Architecture"**, version 1.0, 1999.

[OAKS98] Oaks, S. - **Java Security**. O´Reilly, 1998

[PERK01] Perkins, C.E. - **Ad Hoc Networking** - Addison-Wesley, 2001.

[STAL98] Stallings, W. - **Cryptography and Network Security-Principles and Practice** - Prentice Hall, second edition, 1998.

[TORR85] Torrieri, D. J. - **Principles of Secure Communication Systems.** Norwood, MA: Artech House, 1985.

[TRÄS00] Träskbäck, M. - **Security of Bluetooth: An overview of Bluetooth Security** – 2000.

[VAIN00] Vainio, Juha T. - **Bluetooth Security** - 2000-05-25 [referred 2001-07-25], http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[ZHOU99] Zhou, L.; Haas, Z. - **Securing Ad-Hoc Networks**, IEEE Network. Nov/Dec. 1999.