MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
SECRETARIA DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

MYRNA CECÍLIA MARTINS DOS SANTOS

ANÁLISE FORMAL DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES CELULARES

Rio de Janeiro
2002

INSTITUTO MILITAR DE ENGENHARIA

MYRNA CECÍLIA MARTINS DOS SANTOS

ANÁLISE FORMAL DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES CELULARES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Ciências em Sistemas e Computação.

Orientador: José Ferreira de Rezende – D.C.
Co-orientador: José Antônio Moreira Xexéo – D.C.

Rio de Janeiro
2002

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 – Praia Vermelha
Rio de Janeiro – RJ CEP: 22290-270

S231 Santos, Myrna Cecília Martins dos.
Análise formal de protocolos de autenticação para redes celulares / Myrna Cecília Martins dos Santos. -- Rio de Janeiro : Instituto Militar de Engenharia, 2002.
127 p. : il.,tab.

Dissertação (mestrado) – Instituto Militar de Engenharia – Rio de Janeiro, 2002.

1. Criptografia. 2. Análise de Protocolos. 3. Redes Celulares. I. Instituto Militar de Engenharia. II. Título.

CDD 004.62

INSTITUTO MILITAR DE ENGENHARIA

MYRNA CECÍLIA MARTINS DOS SANTOS

ANÁLISE FORMAL DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES CELULARES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Computação e Sistemas do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Ciências em Sistemas e Computação.

Orientador: Prof. José Ferreira de Rezende – D.C..

Co-orientador: Prof. José Antônio Moreira Xexéo – D.C.

Aprovada em 27 de Junho de 2002 pela seguinte Banca Examinadora:

_____

Prof José Ferreira de Rezende – D.C. da COPPE – Presidente

_____

Prof José Antônio Moreira Xexéo – D. C. do IME

_____

Paulo Cesar Coelho Ferreira - *Docteur* do PRODERJ

Rio de Janeiro

2002

A Deus por iluminar meu caminho, aos meus pais, minhas irmãs, meu irmão e a meu futuro esposo, pelo amor, compreensão e força, fazendo com que eu acreditasse no meu potencial para vencer mais esta batalha.

AGRADECIMENTOS

A meus pais pelo amor incondicional, pelos exemplos de vida e pela oportunidade de me deixar crescer e poder agradecer em forma de vitórias as nossas conquistas.

A minhas irmãs pela confiança na irmã mais velha, pelo carinho, compreensão e apoio.

A meu irmão de coração pela força e por ser uma pessoa muito especial.

Pelas rezas e preocupações da vó Dina e do vô João.

A meu futuro esposo Glauco, pelo seu amor, amizade, cumplicidade, ajuda, por me acalmar e dar força nas horas mais difíceis.

Com certeza a presença de cada um de vocês foi fundamental nesta etapa.

A meus companheiros de turma, que se tornaram grandes amigos: Andres Level, Cadu, Thiago, Paulo Renato (NetStreet Boys) e Alan que dividiram os momentos mais "dramáticos" e mais divertidos no IME.

A Genelice e Gilberto, que apesar de terem seguido áreas diferentes, estiveram sempre presentes dando muita força.

Ao Glauter, pelo apoio, carisma e pelas "tiradas" engraçadas para levantar o astral.

Às professoras Cláudia Justel, Ana Maria e Lilian Markenzon, pela preocupação, por ouvirem minhas queixas e pelo apoio irrestrito que foi importante nesta caminhada. Vocês foram meus anjos da guarda.

Em especial ao professor Xexéo, pelos ensinamentos de criptografia, segurança e, principalmente pela amizade conquistada.

E ao professor José Ferreira de Rezende, pela sua confiança, coragem em dar prosseguimento ao trabalho, disponibilidade e atenção dispensada.

O apoio de vocês e a orientação prestada foram essenciais para a concretização deste trabalho.

Ao Departamento de Engenharia de Sistemas do Instituto Militar de Engenharia pela oportunidade. E ao Cel. Paulo Roberto de Lira Gondim, por dar inicío a orientação do meu trabalho**.**

SUMÁRIO

LISTA DE ILUSTRAÇÕES 08
LISTA DE TABELAS 09
LISTA DE ABREVIATURAS E SÍMBOLOS 10
LISTA DE SIGLAS 12

1. INTRODUÇÃO 16
1.1. Motivação 16
1.2. Objetivo do Trabalho 17
1.3. Organização do Trabalho 18

2. SEGURANÇA E REDES SEM FIO 20
2.1. Introdução 20
2.2. Conceitos Básicos de Segurança 22
2.2.1. Criptografia 22
2.2.2. Tipos de Sistemas Criptográficos 23
2.2.3. Assinatura Digital 26
2.2.4. Autenticação 29
2.2.5. Técnicas Para Distribuição de Chaves 31
2.3. Conceitos Básicos de Redes Sem Fio 33
2.3.1. Componentes Básicos de um Sistema Móvel Celular 34
2.3.2. Desenvolvimento da Rede Móvel 36
2.3.2.1. Primeira Geração de Redes Sem Fio 36
2.3.2.2. Segunda Geração de Redes Sem Fio 37
2.3.2.3. Terceira Geraçao de Redes Sem Fio 38
2.4. Segurança em Redes Móveis 39
2.5. Métodos Formais 41
2.5.1. Métodos Baseados em Linguagens de Verificação 43
2.5.2. Métodos Baseados em Cenários (Sistemas Especialistas) 44
2.5.3. Métodos Baseados em Lógicas Modais 45
2.5.4. Métodos Basados em Sistemas Algébricos 46
2.6. Considerações Finais 47

3. COMPARAÇÃO ENTRE AS LÓGICAS BAN E GNY 49
3.1. Introdução 49
3.2. Protocolo para Distribuição de Chaves Needham-Schroeder 51
3.3. Descrição dos Métodos 53

3.3.1. Lógica BAN 53
3.3.1.1. Notação Básica 55
3.3.1.2. Postulados Lógicos 57
3.3.1.3. Análise Formal 60
3.3.2. Lógica GNY 66
3.3.2.1. Notação Básica 67
3.3.2.2. Postulados Lógicos 68
3.3.2.3. Análise Formal 73
3.4. Comparação e Considerações Finais 83

4. ANÁLISE DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDE CELULAR 85
4.1. Introdução 85
4.1.1. Propósitos de Segurança 86
4.1.2. Notação Básica 87
4.1.3. Postulados Lógicos 89
4.2. GSM 91
4.2.1. Objetivos do Protocolo 93
4.2.2. Fluxo de Mensagens 94
4.2.3. Análise Formal 96
4.3. CDPD 101
4.3.1. Objetivos do Protocolo 102
4.3.2. Fluxo de Mensagens 103
4.3.3. Análise Formal 104
4.4. UMTS 109
4.4.1. Objetivos do Protocolo 111
4.4.2. Fluxo de Mensagens 112
4.4.3. Análise Formal 113
4.5. Considerações Finais 116

5. CONCLUSÕES E TRABALHOS FUTUROS 118
5.1. Conclusão 118
5.2. Trabalhos Futuros 120

6. REFERÊNCIAS BILIOGRÁFICAS 122

LISTA DE ILUSTRAÇÕES

FIG. 2.1 Ciframento e Deciframento com uma única chave 24
FIG. 2.2 Ciframento e Deciframento com duas chaves distintas 25
FIG. 2.3 Assinatura Digital usando o Sistema de Chave Pública 27
FIG. 2.4 Função *Hash* 28
FIG. 2.5 Distribuição de Chaves Diffie-Hellman 32
FIG. 2.6 Ambiente de Comunicação Móvel Celular 35
FIG. 3.1 Protocolo de Distribuição de Chaves Needham-Schroeder 52
FIG. 4.1 Arquitetura da Rede GSM 92
FIG. 4.2 Protocolo de Autenticação do GSM 94
FIG. 4.3 Protocolo de Autenticação do GSM (móvel fora da área de registro) 95
FIG. 4.4 Arquitetura da Rede CDPD 101
FIG. 4.5 Protocolo de Autenticação do CDPD 103
FIG. 4.6 Arquitetura da Rede UMTS 110
FIG. 4.7 Protocolo de Autenticação do UMTS 112

LISTA DE TABELAS

TAB. 2.1 Objetivos dos Protocolos Criptográficos 21
TAB. 2.2 Serviços de Segurança 39
TAB. 3.1 Comparação das Conclusões entre a Lógica BAN e GNY 81

LISTA DE ABREVIATURAS E SÍMBOLOS

ABREVIATURAS

1G	Primeira Geração de Redes Sem Fio
2G	Segunda Seração de Redes Sem Fio
3G	Terceira Geração de Redes Sem Fio
AC	Autoridade Central
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
F-ES	Fixed End System
HLR	Home Location Register
HN	Home Network
ICP-Gov	Infra-estrutura de Chaves Públicas do Poder Executivo Federal
MDBS	Mobile Data Base Station
M-ES	Mobile End System
MHF	Mobile Home Function
MS	Mobile Station
MSC	Mobile Switching Center
MSF	Mobile Serving Function
NEI	Network Entity Identifiers
VLR	Visitor Location Register
VN	Visitor Network

SÍMBOLOS

$\{X\}_k$	fórmula X cifrada com a chave k
<X>Y	combinação da fórmula X com a fórmula Y
N_X	número aleatório (ou identificador único) gerado por X

K_{XY}	chave secreta compartilhada entre X e Y (sistema criptográfico de chave simétrica)
K_X	chave pública de X (sistema criptográfico de chave assimétrica)
K_X^{-1}	chave privada de X (sistema criptográfico de chave assimétrica)
$P \models X$	P acredita em X
$P \lhd X$	P recebe X
$P \vdash\!\sim X$	P disse X
$P \Rightarrow X$	P tem jurisdição sobre X
#(X)	A fórmula X é nova
$P \leftrightarrow^{k} Q$	P e Q compartilhadam a chave secreta k
$\mapsto^{k} P$	P possui como chave pública k (k^{-1} = chave privada)
$P \rightleftharpoons^{X} Q$	A fórmula X é um segredo conhecido somente por P e Q
P ∋ X	P possui a fórmula X
$P \models ø(X)$	P acredita que reconhece X

LISTA DE SIGLAS

AES	Advanced Encryption Standards
AMPS	Advanced Mobile Phone Services
ARN	Authentication Record Number
ASN	Authentication Sequence Number
BAN	Burrows, Abadi e Needham
B-ISDN	Broadband Integrated Service Digital Network
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CSP	Communicating Sequential Processes
DECT	Digital Enhanced Cordless Telephony
DES	American Data Encryption Standard
FDMA	Frequency Division Multiple Access
FDR	Failure Divergence's Refinement
FPLMTS	Future Public Land Mobile Telecommunication Systems
GNY	Gong, Needham e Yahalom
GSM	Global System for Mobile Communications
HOL	Higher Order Logic
IDEA	International Data Encryption Algorithm
IMT-2000	International Telecommunication System
ISO	International Standards Organization
ITU	International Telecommunications Union
LOTOS	Language of Temporal Ordering Specification
MD5	Message Digest nº 5
NRL	Navy Research Laboratory's Protocol Analyzer
NSA	National Security Agency
PCN	Personal Communication Network
PCS	Personal Communication Systems
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RSA	Rivest, Shamir e Adleman
SHA	Secure Hash Algorithm
SS7	Signaling System nº 7

TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunications System

RESUMO

O crescimento extraordinário que tem ocorrido nesta década nas áreas de comunicação celular, redes locais sem fio e serviços via satélite permitirá que informações e recursos possam ser acessados e utilizados em qualquer lugar e em qualquer momento. Por isso, a preocupação com a segurança das informações torna-se cada vez mais importante.

O livre acesso aos meios sem fio, expõe o conteúdo da comunicação sobre os enlaces entre uma unidade móvel e a rede cabeada ou mesmo entre unidades móveis, dando ao intruso a oportunidade de se passar por um assinante legítimo e obter informações sigilosas, como por exemplo, senhas e documentos importantes.

Para garantir a segurança das informações vários protocolos foram desenvolvidos. Esses protocolos utilizam técnicas de criptografia para fornecerem: o sigilo do conteúdo das mensagens e da identidade do usuário/entidade, a autenticação dos participantes da comunicação, a integridade dos dados e o não-repúdio.

O problema é que esses protocolos criptográficos estão sujeitos a erros no desenvolvimento, erros estes que podem ocorrer em qualquer uma das fases de seu projeto e, conseqüentemente, tornando-os vulneráveis a ataques. Foram criados então, métodos formais que têm a função de analisar e verificar se os objetivos propostos pelos autores dos protocolos foram alcançados.

Este trabalho tem como finalidade mostrar a importância do emprego de métodos formais nos protocolos criptográficos. Para isso, foi realizada a análise de três protocolos de autenticação para o ambiente celular: GSM, CDPD e UMTS, utilizando uma das categorias de métodos formais, denominada lógica BAN.

ABSTRACT

The extraordinary growth of cellular communication, wireless local networks and satellite services in this decade will allow the access and use of data and resources anywhere and any moment. Because of this, the worry with security becomes more and more important.

The free access to the wireless medium exposes all the communication data on the links between a mobile unit and the wired network or even between mobile units, leaving an intruder fakes a legitimate signer and get privacy data as passwords and important documents.

To keep the data security several protocols were developed. These protocols use cryptography technicals to provide: the privacy of data messages and user/entity id, the authentication to the participants of communication, the data integrity and nonrepudiation.

The problem is these protocols are not free of development mistakes. These kind of mistakes may occur in any phases of its project, leaving the protocol vulnerable to attack. This way, formal methods were created. They have the function of analyze and verify if the goals proposed by the authors of the protocol were successfully achieved.

This work has the finality to show the importance of using formal methods in the cryptographics protocols. In this work it was realized an analysis of three authentication protocols to the cellular environment: GSM, CDPD and UMTS, using one of the formal methods categories, called BAN logic.

1. INTRODUÇÃO

1.1. MOTIVAÇÃO

Um dos setores de maior crescimento da tecnologia de informação é o setor de comunicações sem fio. Nos dias atuais existem milhões de usuários de telefones celulares no mundo. Estima-se que em 2005, cinqüenta por cento de todas as comunicações irão envolver enlaces sem fio (ANATEL, 2002).

A Internet também apresenta um número crescente de aplicações. Assim, serviços que antes exigiam a presença física dos indivíduos, atualmente são disponíveis pela Internet, como compras *on-line* e movimentações bancárias. Estes serviços já atingiram o setor sem fio, onde podem ser realizados através de terminais móveis (*m-commerce*)[1]. Como conseqüência há um aumento do número de crimes relacionados às telecomunicações causando grande perda de capital.

Nas redes de comunicação as mensagens trocadas entre as entidades (computadores, terminais e usuários) podem ser interceptadas por um intruso. E o ambiente sem fio é o mais vulnerável já que as redes usam o ar como meio de transmissão. Qualquer um com um receptor apropriado pode interceptar as mensagens sem ser detectado. Como resultado, informações importantes, como senhas, chaves ou documentos secretos correm o risco de ficarem expostas, a menos que estejam protegidas.

Para garantir a segurança das informações vários protocolos criptográficos foram desenvolvidos. Esses protocolos utilizam técnicas de criptografia para atingirem seus principais objetivos: sigilo do conteúdo da mensagem ou da identidade do usuário, autenticação dos participantes na comunicação, integridade dos dados ou mensagens e não-repúdio.

---

[1] *m-commerce* – Comércio eletrônico móvel.

1.2. OBJETIVO DO TRABALHO

Existem dois tipos de sistemas criptográficos que permitem que as partes se comuniquem seguramente: sistema criptográfico de chave simétrica e sistema criptográfico de chave pública. No sistema criptográfico de chave simétrica, é requerido que o transmissor e o receptor compartilhem, em segredo, a mesma chave. Nos sistemas criptográficos de chave pública, cada usuário possui um par de chaves privada/pública. As mensagens transmitidas para um determinado usuário são cifradas com a chave pública deste usuário (conhecida por todos os integrantes da rede) e decifradas com a chave privada[2] do mesmo usuário (só ele conhece). Estes sistemas são descritos com maiores detalhes no segundo capítulo.

Além dos aspectos de segurança devem ser consideradas também a eficiência e a vazão (*throughput*) em aplicações práticas. Um ambiente sem fio normalmente requer dispositivos de baixa potência e de rápida computação, o que implica que o número de mensagens trocadas e a complexidade das operações de cifrамento/decifрamento devem ser mantidos tão baixos quanto possíveis.

Os protocolos criptográficos são utilizados para fornecer comunicações seguras sobre a rede. No entanto, estão sujeitos a erros no desenvolvimento, erros estes que podem ocorrer em qualquer uma das fases do seu projeto (especificação, construção e verificação). Mesmo que um protocolo criptográfico seja desenvolvido de forma correta, ou seja, os requisitos sejam os reais requisitos do usuário e o projeto seja realizado de acordo com eles, ainda assim, não existirá a garantia de que o protocolo realizará os serviços de segurança para o qual foi projetado, já que na utilização de um protocolo criptográfico, deve ser levada em conta a ação de intrusos que podem atacar os protocolos das seguintes formas: pela substituição, modificação, exclusão ou criação de mensagens, ou pelo ataque aos algoritmos criptográficos utilizados.

---

[2] Neste trabalho, para fazer a distinção entre chave privada e chave secreta, será sempre utilizado chave privada para fazer referência ao sistema criptográfico de chave assimétrica e chave secreta como referência ao sistema criptográfico de chave simétrica.

Durante a última década, vários métodos formais têm sido propostos a fim de analisar e projetar protocolos criptográficos. Tais métodos formais dividem-se basicamente em: métodos baseados em linguagens de verificação, métodos baseados em sistemas especialistas, métodos baseados em lógicas modais e métodos baseados em modelos algébricos (MEADOWS, 1995), (GRITZALIS, SPINELLIS e GEORGIADIS, 1999), (BUTTYÁN, 1999) e (RUBIN e HONEYMAN, 1993).

O principal objetivo deste trabalho é mostrar a importância do emprego de métodos formais no planejamento de protocolos criptográficos. Esses métodos devem ser utilizados não só pelos analistas, mas também pelos projetistas de protocolos a fim de permitir a correta implementação dos mesmos. Para isso, foi feita uma comparação entre as lógicas BAN (Burrows, Abadi e Needham, seus criadores) e GNY (Gong, Needham e Yahalom) e depois realizada uma avaliação empregando a lógica formal BAN aos protocolos de autenticação do ambiente celular.

1.3. ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em cinco capítulos, sendo o primeiro a introdução e os restantes descritos a seguir:

Capítulo 2 – Segurança e Redes sem Fio – revê a bibliografia sobre os conceitos básicos de segurança, redes móveis celulares e resume os métodos formais aplicados na análise de protocolos criptográficos.

Capítulo 3 – Comparação entre as Lógicas BAN e GNY – compara a eficiência e a flexibilidade dos dois métodos baseados em lógicas modais, analisando o protocolo de distribuição de chaves Needham-Schroeder.

Capítulo 4 – Análise de Protocolos de Autenticação para Rede Celular – realiza uma avaliação dos protocolos de autenticação dos seguintes sistemas de comunicação celular: GSM (*Global System for Mobile Communications*), CDPD (*Cellular Digital*

Packet Data) e UMTS (*Universal Mobile Telecommunications System*) empregando a lógica BAN.

Capítulo 5 – Conclusão e Trabalhos Futuros – apresenta as principais conclusões desta dissertação e sugestões para trabalhos futuros.

2. SEGURANÇA E REDES SEM FIO

2.1. INTRODUÇÃO

A área de telecomunicações tem passado, nesta última década, por um significativo crescimento do número de usuários de redes de comunicação móveis, permitindo a mobilidade dos terminais e a quase total independência de localização. O emprego de terminais móveis representa um desafio na utilização de protocolos usados tradicionalmente pela computação convencional em redes fixas.

Com a crescente demanda por serviços de comunicação móvel, a segurança das informações que trafegam na rede torna-se cada vez mais importante. Empresas, áreas governamentais e, principalmente, as áreas militares, sentem-se vulneráveis quando a segurança é ignorada.

Apesar das redes sem fio possuírem vantagens sobre as redes cabeadas, incluindo a eliminação de custos de cabeamento e o aumento da mobilidade do usuário, elas apresentam sérios problemas de segurança. Ao contrário das redes cabeadas, onde o acesso ao meio de transmissão é dificultado, as redes sem fio usam o ar como meio de transmissão. Qualquer indivíduo com um receptor apropriado pode ter acesso aos dados transmitidos, como senhas e documentos importantes e secretos.

A mobilidade também traz problemas já que um computador móvel pode se conectar à rede em locais diferentes, as quais podem ou não ser confiáveis, dando ao intruso a oportunidade de ler, apagar e alterar as mensagens que trafegam na rede, ou até mesmo de se passar como um assinante legítimo e realizar chamadas gratuitas.

Para garantir a segurança das informações, foram desenvolvidos protocolos criptográficos. Um protocolo é um conjunto de regras e convenções que definem uma estrutura de comunicação entre dois ou mais integrantes da rede (LOWE, 1997). Nos protocolos criptográficos, pelo menos uma parte da mensagem é

cifrada[3], a fim de estabelecerem comunicações seguras sobre redes inseguras (BRACKIN, 1999) e (MONNIAUX, 1998). Estes protocolos utilizam técnicas de criptografia para alcançarem os objetivos (DECRETO LEI 3587) mostrados na TAB. 2.1.

TAB. 2.1 – Objetivos dos Protocolos Criptográficos

Objetivos	Descrição
Sigilo	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas às partes autorizadas.
Integridade	Garantir que a informação (ou mensagem) não foi alterada durante a sua transferência do emissor da mensagem para o seu receptor.
Autenticação	Confirmar a identidade de uma pessoa ou entidade ou garantir a fonte de uma mensagem.
Não-repúdio	Garantir que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gerar.

As seções deste capítulo foram estruturadas de forma a permitir que se tenha uma visão geral dos conceitos básicos de segurança e de redes celulares. Na seção 2.2 são descritos os conceitos básicos de criptografia para o planejamento de um protocolo de segurança; na seção 2.3 é realizado um resumo sobre o ambiente sem fio infra-estruturado e como a rede se desenvolveu nos últimos anos (primeira, segunda e terceira geração); na seção 2.4 são mostrados os serviços de segurança que os protocolos criptográficos devem fornecer; na seção 2.5 é feito um resumo dos métodos formais para a análise de protocolos criptográficos e na seção 2.6 são realizadas as considerações finais do capítulo.

[3] Uma mensagem é dita cifrada quando passa por um processo de codificação, definido por um método de criptografia, que modifica o texto original da mensagem (texto em claro), gerando um texto cifrado na origem (DIFFIE e HELLMAN, 1979).

2.2. CONCEITOS BÁSICOS DE SEGURANÇA

A segurança está relacionada à necessidade de proteção contra o acesso ou a manipulação, intencional ou não, de informações confidenciais por pessoas não autorizadas (SOARES, LEMOS e COLCHER, 1995).

Muitas vezes chega-se a conclusão errônea que a criptografia fornece segurança, enquanto que na realidade a criptografia é uma ferramenta que pode prover os requerimentos de segurança, como por exemplo, sigilo, autenticação, integridade e não-repúdio (MYRVANG, 2000).

Esta seção faz um resumo dos principais conceitos de criptografia utilizados no decorrer deste trabalho, tais como, tipos de sistemas criptográficos, autenticação e distribuição de chaves. Estes conceitos são empregados na implementação dos protocolos, com o objetivo de prover a segurança das informações que trafegam na rede.

2.2.1. CRIPTOGRAFIA

Criptografia pode ser definida como a arte e a ciência de manter mensagens secretas (SCHNEIER, 1996). Ela surgiu da necessidade de enviar informações importantes através de meios de comunicação não confiáveis, ou seja, em meios onde não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo) ou para modificá-lo (intruso ativo). Por isso é empregado um método que modifica o texto original da mensagem (texto em claro), gerando um texto cifrado na origem, através de um processo de codificação definido por um método de criptografia. O texto (ou a mensagem) cifrado é então transmitido e, no destino, o processo inverso ocorre, isto é, o método de criptografia é aplicado agora para decifrar o texto cifrado transformando-o no texto em claro original (DIFFIE e HELLMAN, 1976).

O processo para converter o texto em claro em texto cifrado é chamado de ciframento. O deciframento é o processo contrário, ou seja, obtém o texto em claro original a partir do texto cifrado.

O ciframento e o deciframento são realizados de acordo com os algoritmos criptográficos, que são funções matemáticas usadas para cifrar e decifrar. Estes algoritmos dependem de um pedaço adicional de informação, denominado chave, que é combinado com o texto em claro para obter o texto cifrado ou vice-versa. Um exemplo básico de um algoritmo de ciframento é aquele que através de uma operação de OU-EXCLUSIVO combina uma chave de tamanho fixo com cada bloco do texto em claro para gerar um texto cifrado. Para decifrar uma mensagem assim cifrada, o receptor precisa somente inverter o processo utilizando a mesma chave (DENNING, 1982).

Uma das condições para que um algoritmo criptográfico seja considerado seguro, é publicá-lo para que seja criptoanalisado[4], e, por isso, diz-se que a segurança não está nos detalhes dos algoritmos e sim na manutenção do segredo da chave.

2.2.2. TIPOS DE SISTEMAS CRIPTOGRÁFICOS

Um sistema criptográfico é um sistema com todos os possíveis textos em claro, textos cifrados e chaves, que podem permitir que as partes se comuniquem seguramente. Existem dois tipos de sistemas criptográficos: o sistema de chave simétrica e o sistema de chave assimétrica. As principais diferenças entre eles estão na quantidade de chaves e nos algoritmos criptográficos utilizados (MYRVANG, 2000).

No sistema criptográfico de chave simétrica, também chamado de sistema de chave secreta, chave compartilhada ou chave única, o ciframento e o deciframento utilizam a mesma chave, e como essas transformações (ciframento e deciframento) são facilmente derivadas uma da outra, uma chave secreta comum tem que ser

[4] Criptoanálise é a arte de solucionar mensagens cifradas (TANEMBAUM, 1996).

compartilhada entre as partes, com antecedência, por algum canal ou meio seguro. Estas operações (ciframento e deciframento) são mostradas na FIG. 2.1 a seguir.

Notação utilizada nas FIGs. 2.1, 2.2 e 2.3

C = Ciframento
D = Deciframento
M = Texto em claro
T = Texto cifrado

s = chave secreta
p = chave pública
k = chave privada
$C_s(X)$ = ciframento de **X** usando a chave secreta **s**
$D_s(X)$ = deciframento de **X** usando a chave secreta **s**

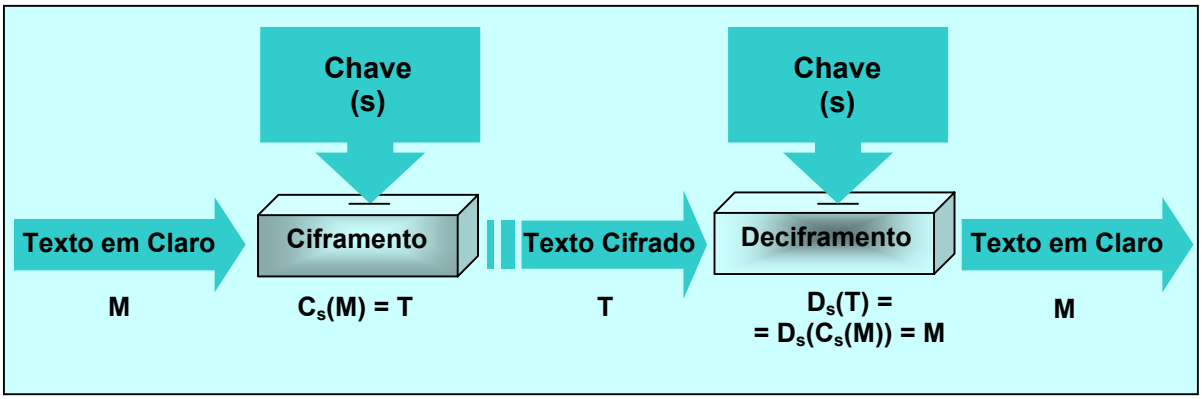

FIG. 2.1 – Ciframento e Deciframento com uma única chave

A segurança de um sistema simétrico está no gerenciamento e na manutenção do segredo da chave. Divulgá-la significa que qualquer um pode cifrar e decifrar as mensagens. Para que a comunicação permaneça secreta, a chave deve, então, ser mantida em segredo.

Os sistemas simétricos podem ser divididos em duas categorias: os que operam o texto em claro bit a bit (ou byte a byte), ou seja, operam um bit a cada unidade de tempo por vez e, por isso, são chamados de cifra de fluxo (*stream cipher*); e os que manipulam o texto em claro em grupos de bits. Estes grupos de bits são chamados de blocos e os algoritmos são conhecidos como cifra de blocos (*blocks cipher*) (OORSCHOT, VANSTONE e MENEZES, 1996). Os sistemas criptográficos de chave simétrica mais conhecidos são: o DES (*American Data Encryption Standard*) (STINSON, 1995), o IDEA (*International Data Encryption Algorithm*) (TANEMBAUM, 1996) e recentemente, o AES (*Advanced Encryption Standard*) (DAEMEN e RIJMEN, 2001).

O sistema criptográfico de chave assimétrica ou chave pública baseia-se em chaves distintas para o ciframento e o deciframento, não sendo computacionalmente fácil determinar a chave de deciframento (chave privada) a partir da chave de ciframento (chave pública). Cada usuário possui um par de chaves, uma pública e uma privada. As chaves públicas de todos os usuários podem ser publicadas em diretórios abertos, facilitando a comunicação entre eles, mas a privada só é conhecida pelo seu próprio dono (DIFFIE e HELLMAN, 1976).

Outra função útil fornecida pelo sistema de chave assimétrica é a assinatura digital (seção 2.2.3). Os sistemas criptográficos de chave assimétrica mais conhecidos são: o RSA (Ron Rivest, Adi Shamir e Leonard Adleman, seus criadores) (SEBERRY e PIEPRZYK, 1994), o Sistema de Criptografia de Curva Elíptica (GALBRAITH, 1997) e o Sistema de Criptografia ElGamal (STINSON, 1995). A FIG. 2.2, a seguir, mostra o ciframento e o deciframento utilizando duas chaves distintas.

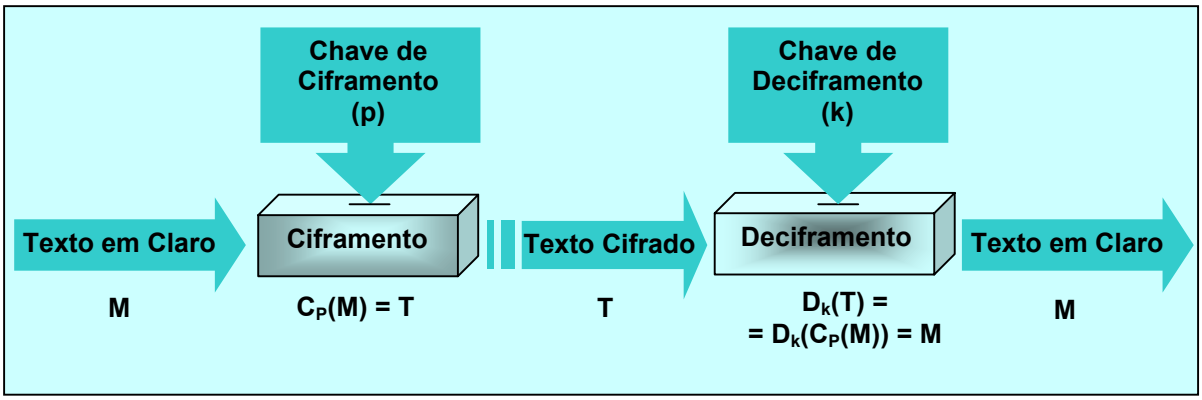

FIG. 2.2 – Ciframento e Deciframento com duas chaves distintas

Os sistemas criptográficos são empregados para ocultar o conteúdo das mensagens trocadas entre as partes envolvidas na comunicação e os protocolos para distribuição de chaves e autenticação podem ser construídos com base em um ou mais dos sistemas citados.

No planejamento de protocolos de segurança para o ambiente sem fio, uma das preocupações é a escolha do sistema criptográfico, por causa do consumo de energia. Por isso, a quantidade de mensagens trocadas entre as partes e as computações realizadas para o cálculo das chaves de sessão e no ciframento e deciframento das mensagens devem ser minimizadas.

Em (BASYOUNI e TAVARES, 1996) e (PATIYOOT e SHEPHERD, 1999) são realizadas comparações entre esses sistemas no ambiente de comunicação sem fio. A principal conclusão é que os protocolos que utilizam o sistema criptográfico de chave assimétrica não possuem nenhuma vantagem clara sobre os de chave simétrica, até porque os algoritmos de chave pública (não estão sendo considerados os algoritmos de curva elíptica)[5] são mais lentos na computação do que os de chave simétrica (que são, geralmente, três vezes mais rápidos), as implementações de *hardware* consomem maior potência e o número de mensagens trocadas pela rede, normalmente, é maior do que nos sistemas criptográficos de chave secreta.

Uma alternativa é usar sistemas híbridos que aproveitam vantagens de ambos: a alta eficiência do sistema criptográfico de chave assimétrica para a distribuição de chaves e a rapidez e baixa computação do sistema criptográfico de chave simétrica para o ciframento e o deciframento das informações. Como exemplo, podem ser citados os trabalhos de (BELLER, CHANG e YACOBI, 1993) que propuseram três protocolos com estes conceitos e os de (AZIZ e DIFFIE, 1994) que desenvolveram um protocolo de autenticação para o ambiente sem fio que usa o sistema criptográfico de chave pública para a criação da chave de sessão e o sistema criptográfico de chave secreta para o ciframento e deciframento das mensagens.

2.2.3. ASSINATURA DIGITAL

A assinatura digital, como o próprio nome sugere, é a análoga eletrônica da assinatura manuscrita mas, ao contrário dela, é, virtualmente, impossível de se forjar (OORSCHOT, VANSTONE e MENEZES, 1996). Ela é formada combinando partes de informações secretas, que pertencem ao remetente, com a mensagem a ser enviada. Quando o receptor receber a mensagem, poderá verificar o seu conteúdo, mas não poderá falsificar a assinatura.

---

[5] Os algoritmos de curvas elípticas são mais rápidos na computação, pois utilizam tamanho de chaves menores. Em (LÓPEZ e DAHAB, 2000) e (AYDOS, YANIK e KOÇ, 2000) foram realizados testes de seus desempenhos no ambiente celular.

A maioria das assinaturas digitais são realizadas pelos sistemas criptográficos de chave pública, embora possam ser utilizados sistemas de chave simétrica. Neste último, torna-se necessária uma terceira parte confiável (Autoridade Central – AC) que irá realizar o gerenciamento de todo o processo.

O mecanismo envolve, basicamente, dois procedimentos: a assinatura (ciframento) da mensagem completa ou apenas de uma parte, utilizando a informação privada (chave secreta) do signatário, e a verificação, onde o receptor usa a informação pública (chave pública) do assinante para o deciframento da mensagem e reconhecimento da assinatura (FIG. 2.3).

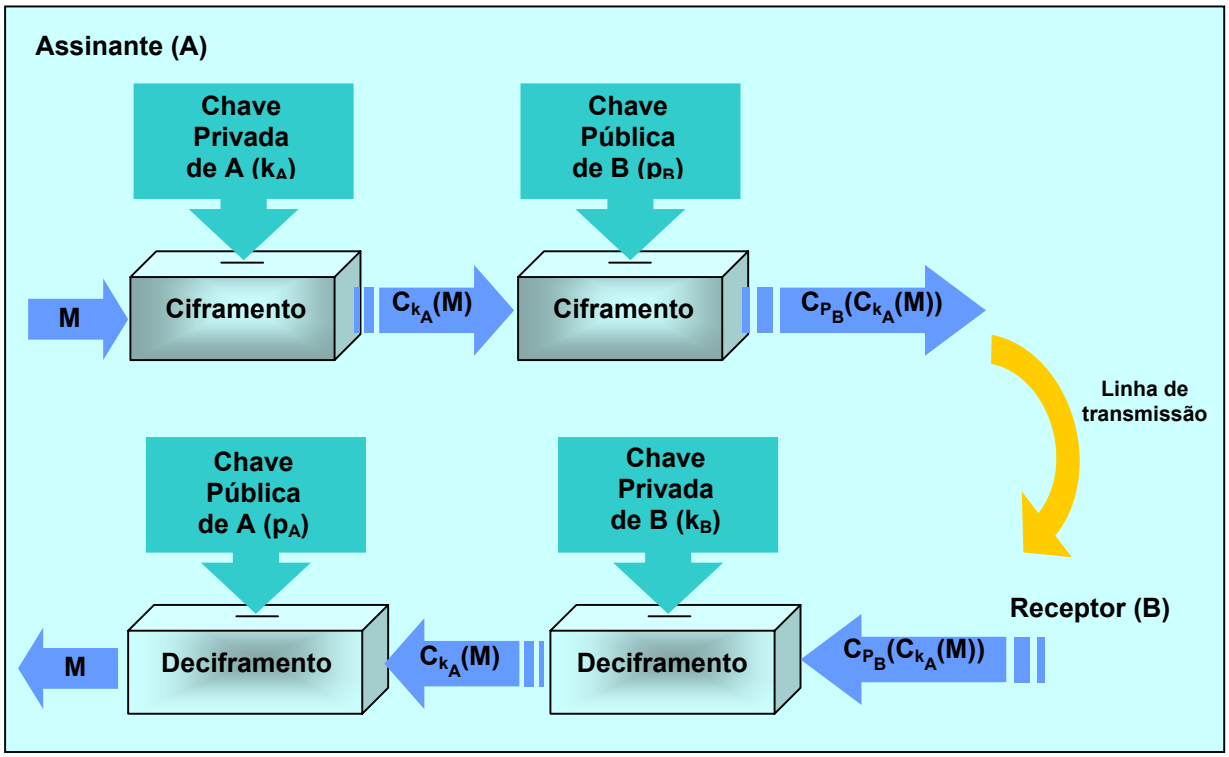

FIG. 2.3 – Assinatura Digital usando o Sistema de Chave Pública

O algoritmo de chave pública RSA é um dos que possui esta propriedade, ou seja, utiliza a chave privada para cifrar e, conseqüentemente, assinar o documento, e usa a chave pública para decifrar, realizando a operação de verificação. Alguns algoritmos são usados somente para gerar assinaturas digitais e não para cifrar mensagens (SEBERRY e PIEPRZYK, 1994).

Como os algoritmos de chave pública são normalmente lentos para cifrar e decifrar a mensagem, torna-se custoso criptografá-la completamente. Ao invés disso pode ser aplicada outra técnica comum para gerar assinaturas digitais, que envolve uma função *hash* unidirecional. A função *hash* é uma função matemática, que pega como entrada um trecho qualquer do texto em claro (P) de tamanho variável (chamado pré-imagem) e o converte numa *string* de tamanho fixo, geralmente menor (chamada valor *hash*) (BRANCHAUD, 1997). Essa função *hash*, chamada de compilação de mensagem (*message digest* – MD), possui três propriedades importantes:

a) se a pré-imagem (P) for fornecida, é fácil calcular o valor *hash* associado a ela (MD(P));

b) se o valor *hash* for fornecido (MD(P)), será praticamente impossível calcular a pré-imagem (P);

c) ninguém pode gerar duas mensagens que tenham o mesmo valor *hash*.

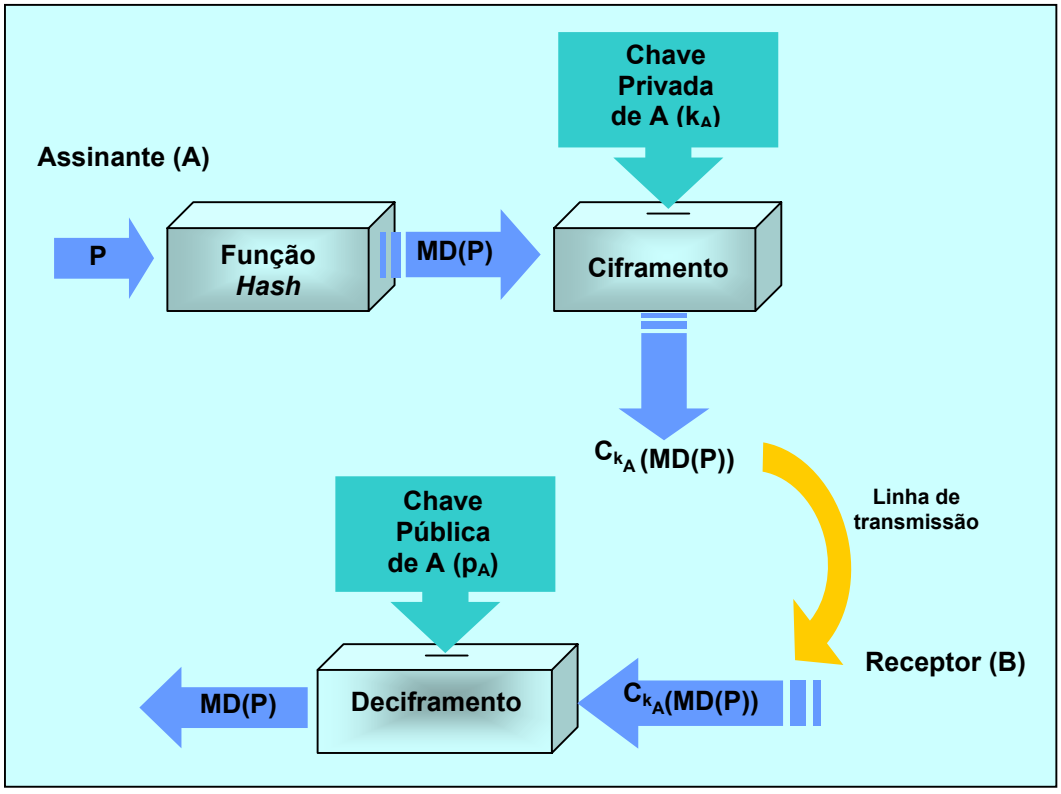

FIG. 2.4 – Função *Hash*

Em vez de assinar toda a mensagem, A calcula o valor *hash*, aplicando MD a P e produzindo (MD(P)). Em seguida, A envia a compilação assinada com sua chave

privada e o texto em claro (M) para B. Se futuramente, B precisar provar que recebeu uma mensagem assinada de A, então ele apresenta a mensagem e o MD(P) recebidos e mostra que o MD(P) só pode ter sido gerado por A, pois B não conhece a chave privada do emissor e não pode produzir a mesma compilação de mensagem a partir do texto em claro M.

Calcular o valor *hash* de uma mensagem, a partir de um trecho do texto em claro, é muito mais rápido do que criptografá-la com um algoritmo de chave pública, agilizando o processo de assinatura digital.

As funções *hash* utilizadas com mais freqüência são MD5, que é a quinta de uma série de funções criadas por Ron Rivest, e SHA (*Secure Hash Algorithm*) desenvolvida pelo NSA (*National Security Agency*) (TANENBAUM, 1996).

A característica essencial do mecanismo de assinatura digital é garantir que uma mensagem assinada só pode ter sido gerada com informações confidenciais do assinante, ou seja, uma vez verificada a assinatura com a chave pública, é possível posteriormente provar para um terceiro (por exemplo, um juiz em um tribunal) que só o proprietário da chave privada poderia ter gerado a mensagem.

2.2.4. AUTENTICAÇÃO

A autenticação é a técnica através da qual um processo (pessoa ou entidade) confirma que seu parceiro na comunicação é quem deve ser e não um impostor ou para garantir a fonte de uma mensagem. Sem ela, um intruso poderia se passar como um determinado usuário e obter acesso não autorizado a informações importantes ou interferir nas operações de outros usuários.

Autenticação não deve ser confundida com autorização, já que são técnicas diferentes, a primeira lida com a questão de determinar se o usuário está ou não se comunicando com um determinado processo e a outra se preocupa com o que o processo em questão está autorizado a fazer.

A autenticação é realizada através dos protocolos de autenticação que podem utilizar os conceitos dos sistemas criptográficos de chave secreta e de chave pública. Ambos, com ou sem uma autoridade central (CLARK e JACOB, 1998).

Os protocolos de autenticação podem ser de dois tipos: unilateral, quando apenas quem solicita o acesso é autenticado, ou mútuo, quando as partes envolvidas na comunicação autenticam-se entre si.

Uma autenticação mútua pode ser apoiada por uma infra-estrutura de chaves públicas (*Public Key Infrastructure* – PKI) na qual uma autoridade central garanta a identidade de cada parte com a emissão de certificados digitais juntamente com mecanismos de autenticação para a identificação do usuário certificado (MYRVANG, 2000). Na sua forma mais simples, uma PKI é um sistema para a publicação das informações das chaves públicas utilizadas no sistema criptográfico de chave assimétrica (BRANCHAUD, 1997) e (ELLISON e SCHNEIER, 2000).

A certificação é a função fundamental de todas as PKIs e um certificado digital é uma declaração assinada digitalmente por uma autoridade central (AC) contendo, alguns atributos, tais como o nome da AC que emitiu o certificado, o nome de um assinante para quem o certificado foi emitido, a chave pública do assinante e o período de validade operacional do certificado (GERCK, 2000).

No Brasil foi elaborado o Decreto Lei nº 3.587 (DECRETO LEI 3587, 2000), sancionado pelo presidente da República no dia 5 de setembro de 2000. O decreto estabelece normas para a instituição da infra-estrutura de chaves públicas do Poder Executivo Federal – ICP-Gov, definindo que sua tecnologia deverá utilizar o sistema criptográfico de chave assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade. Serão usadas duas chaves matematicamente relacionadas, uma pública e outra privada, para a criação de uma assinatura digital que permitirá a realização de transações eletrônicas seguras e a troca de informações sensíveis e classificadas. A portaria também determina a organização do ICP-Gov e trata da criação de uma agência governamental para estabelecer e administrar políticas para a formação e atuação de autoridades certificadoras e autoridades de registro.

A organização da ICP-Gov foi baseada no X.509 (MITCHELL, WALKER e RUSH, 1999) e (LEE e CHANG, 1997). O X.509 é um *framework* de autenticação desenvolvido para suportar os serviços do diretório X.500. Tanto o X.509 como o X.500 são partes da série X, de padrões internacionais, propostos pela ISO (*International Standards Organization*) e ITU (*International Telecommunications Union*). O padrão X.500 fornece serviços de diretórios em grandes redes de

computadores e o X.509 fornece uma infra-estrutura de chave pública para autenticação dos serviços X.500.

Além de confirmar a identidade das entidades, o protocolo de autenticação deve estabelecer uma chave que deverá ser usada pelas partes durante a comunicação. A chave gerada para uma sessão de comunicação particular denomina-se chave de sessão compartilhada. É interessante que essa chave seja temporária, ou seja, trocada a cada sessão, pois minimiza o volume de tráfego provocado pelo envio das chaves públicas e não dá ao intruso a oportunidade de utilizar uma chave de sessão antiga.

2.2.5. TÉCNICAS PARA DISTRIBUIÇÃO DE CHAVES

Em todos os sistemas criptográficos são necessárias uma ou mais chaves para executar as operações de ciframento e deciframento. Elas nem sempre podem ser negociadas, anteriormente, entre os participantes na comunicação. Parte dos problemas que os protocolos de segurança tentam solucionar é a distribuição dessas chaves, já que deve ser feita de forma segura entre as partes. Esta seção resume algumas das técnicas mais comuns de distribuição de chaves utilizadas pelos protocolos de autenticação.

No sistema criptográfico de chave simétrica, as partes precisam compartilhar a mesma chave para se comunicarem, que deve ser trocada, com antecedência, por algum canal ou meio seguro. Entretanto, é custoso armazenar uma chave para cada participante que pode ser contatado. Por exemplo, numa rede de *n* usuários, um sistema de chave simétrica requer um total de *n(n-1)/2* chaves.

Diffie e Hellman foram os que primeiro propuseram uma solução para o problema de troca de chaves sobre um canal aberto. Os participantes na troca de chaves, escolhem um corpo finito *k* (onde seja computacionalmente impossível de encontrar o logaritmo) e um gerador α do corpo. Se *A* e *B* desejarem trocar uma chave, então *A* escolhe um expoente secreto *a*, calcula α^a e o envia a *B*. Da mesma maneira, *B* escolhe um expoente secreto, *b*, calcula α^b e o envia a *A*. Quando *A* receber α^b poderá calcular $(\alpha^b)^a = \alpha^{ba} = \alpha^{ab}$, pois conhece a. Igualmente, *B* poderá

calcular α^{ab}. Dessa forma, α^{ab} será a chave compartilhada entre eles (FIG. 2.5). A segurança desse esquema depende da dificuldade de calcular logaritmos de um corpo de *Galois* (Problema do Logaritmo Discreto) (DIFFIE e HELLMAN, 1976).

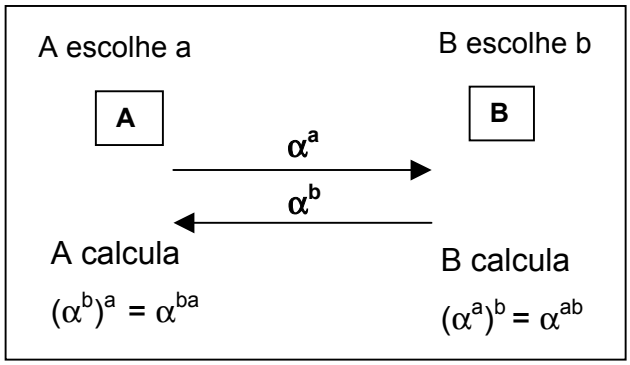

FIG. 2.5 – Distribuição de chaves Diffie-Hellman

Com o sistema criptográfico de chave pública, o número de chaves requeridas para a comunicação é drasticamente reduzido. Numa rede de *n* usuários, serão necessárias *2n* chaves (uma pública e uma privada) para tornar a comunicação segura entre os participantes. Observando de maneira geral, a solução parece simples, já que as chaves públicas de todos os membros podem ficar disponíveis em diretórios abertos e somente a pessoa com posse da correspondente chave privada é que pode decifrar qualquer mensagem cifrada com a respectiva chave pública (BASYOUNI e TAVARES, 1996).

O problema é verificar se o usuário está utilizando a chave pública válida. Uma solução é ter uma terceira parte confiável que assine as chaves públicas a serem distribuídas. Estas chaves assinadas, ou certificados, são usadas para verificar a autenticidade das chaves públicas. Cada usuário precisa somente armazenar uma chave pública, a da autoridade central, já que todas as outras podem ser obtidas dos certificados. Um problema com esse esquema é que se um par de chaves pública/privada estiver comprometido, e se ainda não tiver sido revogado (por exemplo, o intervalo de tempo de atualização da lista de certificados revogados for muito grande) a chave pública poderá ainda permanecer válida no certificado (ELLISON e SCHNEIER, 2000).

Finalmente, existem técnicas de troca de chaves que são facilmente adaptáveis tanto ao sistema criptográfico de chave secreta quanto ao de chave pública. Estas técnicas envolvem o uso de um servidor de distribuição de chaves que pode distribuir chaves públicas ou pode gerar as chaves de sessão. O conceito é semelhante ao esquema de certificado, exceto que a terceira parte confiável, no caso o servidor de distribuição de chaves, é contatado diretamente pelos usuários para a obtenção das chaves. Todos os usuários possuem uma chave pública ou uma chave compartilhada utilizada para contatar o servidor que gera uma chave de sessão para a comunicação. Isto ajuda evitar o problema do servidor ter que armazenar vários pares de chaves compartilhadas para todos os usuários (no caso do sistema de chave simétrica) (BELLER, CHANG e YACOBI, 1993).

2.3. CONCEITOS BÁSICOS DE REDES SEM FIO

Redes sem fio referem-se a redes de computadores que utilizam enlaces sem fio, tais como rádio freqüência e raios infravermelhos para conectar os diversos terminais. Surgiram com a finalidade de superar as limitações de mobilidade e instalação das redes tradicionais (SALLES, 1998).

As comunicações sem fio têm uma longa história de aplicações comerciais e militares. Ultimamente, porém, estão sendo amplamente utilizadas por todos os tipos de usuários – empresários, donas de casa, estudantes e outros, que disponibilizam informações importantes na rede, muitas vezes, sem se preocuparem com os requerimentos de segurança.

Dessa forma, torna-se necessário que sejam projetados métodos que venham garantir o sigilo da identidade e dos dados do usuário e a autenticação que são essenciais ao controle de fraude e na proteção de comunicações privadas contra o acesso ilegal.

Um dos meios de proteção é o emprego de protocolos de autenticação que são desenvolvidos utilizando conceitos criptográficos e que possuem como principal objetivo fornecer a veracidade da identidade das partes que estão se comunicando. Conseqüentemente, um usuário móvel deve ser autenticado pela rede antes de ter a

permissão de acesso. Se o protocolo de autenticação tiver sido projetado para passar informações seguras do usuário móvel para a rede, então a rede também precisa ser autenticada pelo usuário móvel (CLARK e JACOB, 1998) e (PARK, 1997).

Além disso, o conteúdo das mensagens transmitidas através da rede sem fio deve ser cifrado e por isso, as partes envolvidas na comunicação precisam compartilhar uma chave de sessão antes de iniciar a comunicação. O sigilo da identidade do usuário móvel e a sua localização é outra questão de segurança que surge no ambiente de comunicação móvel (RAPPAPORT, 1996). Uma boa solução para garantir o anonimato é dar um apelido (ou uma identidade temporária) ao usuário móvel. Como exemplo, pode-se citar a identidade temporária do assinante móvel (TMSI – *Temporary Mobile Subscriber Identity*) que é um tipo de apelido utilizado pelo GSM.

Além da segurança, existem algumas considerações a serem feitas quando esses protocolos são projetados: o baixo poder computacional das estações móveis, baixa largura de banda e as taxas de erro no canal que são mais altas do que na rede cabeada. Dessa forma, o tamanho e o número de mensagens trocadas devem ser minimizados (PARK, 1996), (PATIYOOT e SHEPHERD, 1998) e (JOSEPH, 2000).

Nesta seção será dada uma breve explicação de como funciona o ambiente de comunicação móvel celular, descrevendo a arquitetura para qual os protocolos de autenticação são projetados. Serão mostrados também os objetivos de segurança que um protocolo criptográfico deve fornecer ao ambiente móvel e o porquê da utilização de métodos formais na avaliação desses protocolos.

2.3.1. COMPONENTES BÁSICOS DE UM SISTEMA MÓVEL CELULAR

O sistema de comunicação móvel celular fornece conexão sem fio a qualquer usuário localizado dentro da área de cobertura de uma estação base. Esse sistema provê alta qualidade de serviço, comparável aos sistemas de telefonia fixa. A alta capacidade é conseguida limitando a cobertura de cada estação base a pequenas

áreas geográficas, denominadas células, tal que os mesmos canais de rádio possam ser reutilizados por outra estação base localizada a alguma distância. Quando o usuário se move de uma célula a outra, é realizado um processo de comutação do usuário de uma estação base ou canal para outro, enquanto a ligação está em andamento. Este processo é chamado de *handoff* (RAPPAPORT, 1996) e (YACOUB, 1993).

A FIG. 2.6 mostra um sistema básico celular. Num sistema de comunicação móvel sem fio existem duas partes fundamentais: os terminais móveis e a rede. A rede consiste em: estações base e centros de comutação móvel (MSC – *Mobile Switching Center*).

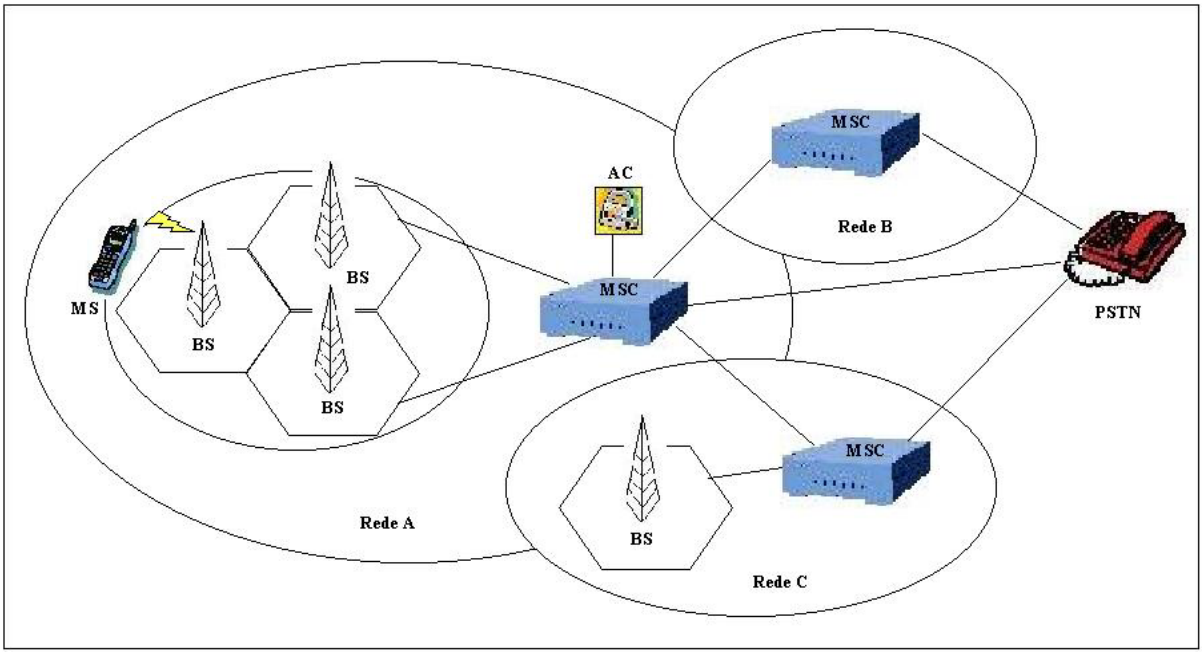

FIG. 2.6 – Ambiente de Comunicação Móvel Celular

As estações (ou terminais) móveis (MS – *Mobile Station*) estão conectadas via rádio a uma estação base (BS – *Base Station*) na rede cabeada, e que, geralmente, está ligada numa rede fixa de alta velocidade (*backbone*). O MSC trabalha como um controlador central, fazendo a interface entre as estações base e a rede de telefonia fixa (PSTN – *Public Switched Telephone Network*). O MSC pode ser responsável por uma grande área metropolitana ou pelo conjunto de pequenas cidades vizinhas. A área controlada por um MSC é denominada por área de serviço. O assinante dentro dessa área é um assinante domiciliar. É possível, porém, que um assinante saia de

sua área de registro, neste caso ele é denominado de *roamer*. As principais tarefas executadas por um MSC incluem: *paging*[6], gerenciamento da localização e dos *handoffs* dos assinantes.

Existem dois tipos de redes: a *Home Network* (HN) e *Visitor Network* (VN). A HN é a rede que registrou o usuário no momento da assinatura. Se a HN do móvel tiver feito algum acordo com uma outra rede móvel, operada por outra fornecedora de serviços móveis, o usuário móvel poderá visitar e ser servido por esta rede (VN).

Algumas vezes, será utilizado o termo rede operadora, rede servidora ou prestadora de serviços, que pode ser a HN ou VN, e que estará prestando serviços ao usuário naquele instante.

O componente mais importante na arquitetura, em relação à segurança, é a Autoridade Central (AC), que armazena as chaves secretas dos assinantes e gera parâmetros de segurança requeridos no processo de autenticação, como o número aleatório utilizado como desafio-resposta (tripla gerada no GSM) (MOLVA, SAMFAT e TSUDIK, 1994). A AC normalmente está ligada ao MSC.

2.3.2. DESENVOLVIMENTO DA REDE MÓVEL

2.3.2.1. PRIMEIRA GERAÇÃO DE REDES SEM FIO

A primeira geração (1G) de redes sem fio é baseada na tecnologia analógica. Como exemplo de primeira geração, pode-se citar o AMPS (*Advanced Mobile Phone Services*) sistema usado nos Estados Unidos. A administração do sistema reside no MSC que mantém todas as informações e o controle de *handoff* da estação móvel. O MSC também executa todas as funções de gerenciamento da rede, tais como a manipulação e o processamento das chamadas, as faturas e a detecção de fraude na rede. O MSC é conectado a PSTN via troncos e comutadores. Os MSCs também são conectados a outros MSCs através de canais de sinalização.

---

[6] *Paging* – sistemas de *paging* são sistemas de comunicação que utilizam mensagens curtas para procurar um terminal móvel ou enviar dados ele (RAPPAPORT,1996).

Nos sistemas celulares modernos, o tráfego de voz é transportado pela PSTN, mas a informação de sinalização usada para fornecer a inicialização das chamadas e informar os MSCs sobre um determinado usuário é transportado pela SS7[7].

A rede 1G fornece voz analógica e ineficiente, além da baixa taxa de transmissão de dados entre a estação base e o usuário móvel. Porém, os sinais de voz, normalmente, são digitalizados usando a multiplexação de divisão por tempo, para transmissão entre a estação base e o MSC e do MSC à PSTN.

2.3.2.2. SEGUNDA GERAÇÃO DE REDES SEM FIO

A segunda geração de sistemas sem fio, 2G, emprega modulação digital e um avançado processamento de chamadas. Como exemplos de segunda geração de sistemas sem fio, podem ser citados o GSM, os padrões digitais: TDMA (*Time Division Multiple Access*) e CDMA (*Code Division Multiple Access*) (padrões da Associação de Indústria de Telecomunicações) e o DECT (*Digital Enhanced Cordless Telephony*) que é o padrão europeu para telefonia sem fio (DORNAN, 2001).

A rede 2G introduziu novas arquiteturas que reduziram a carga computacional do MSC. O GSM, por exemplo, criou o conceito de uma estação base controladora (BSC – *Base Station Controller*) que é inserida entre as várias estações bases e o MSC. Esta mudança na arquitetura permitiu que os dados entre a estação base controladora e o MSC fossem unificados, possibilitando a utilização de diferentes fabricantes e componentes de MSCs e de BSCs. Esta interoperabilidade é uma característica nova para a segunda geração de sistemas sem fio.

Todos os sistemas 2G usam voz e modulação digitais. Os sistemas empregam canais de controle dedicados na interface aérea para trocar, simultaneamente, voz e informações de controle entre o assinante, a estação base e o MSC, enquanto uma chamada está em andamento.

Ao contrário dos sistemas de primeira geração que foram projetados, principalmente, para voz, os de segunda geração foram desenvolvidos para fornecer

[7] SS7 – Rede de Sinalização.

paging e outros serviços de dados como fac-símile e redes de acesso a altas taxas de dados.

O DECT é um exemplo de padrão da segunda geração de telefones sem fio fixo que permite que cada telefone possa se comunicar com qualquer estação base, selecionando automaticamente a que estiver com maior potência de sinal. De maneira geral, a rede 2G foi projetada para reduzir o trabalho computacional das estações base e dos MCSs e fornecer mais flexibilidade na distribuição de canais.

2.3.2.3. TERCEIRA GERAÇÃO DE REDES SEM FIO

Numa primeira instância, a terceira geração de sistemas sem fio, 3G, é uma evolução dos sistemas de segunda geração. A principal função das redes sem fio da terceira geração é fornecer um conjunto de padrões que possam reunir uma grande quantidade de aplicações sem fio e fornecer acesso mundial.

O sistema de terceira geração permitirá o uso da Rede Digital de Serviços Integrados de Banda Larga (B-ISDN – *Broadband Integrated Service Digital Network*) para fornecer acesso às redes de informação, como a Internet. Ela transportará vários tipos de informação (voz, dados e vídeo), operará em diferentes regiões (regiões com população densa ou escassa) e servirá usuários estacionários e também aqueles que estiverem viajando em veículos a alta velocidade.

Os Sistemas de Comunicação Pessoal (PCS) e as Redes de Comunicação Pessoal (PCN) serão utilizadas como referência aos sistemas 3G. Outros nomes para PCS incluem FPLMTS (*Future Public Land Mobile Telecommunication Systems*) para uso mundial e que foi denominado como IMT-2000 (*International Mobile Telecommunication*) e de UMTS (*Universal Mobile Telecommunication System*) para os serviços móveis na Europa.

A telefonia de terceira geração com diferentes protocolos permitirá a integração de uma série de novos dispositivos móveis à rede, enviando, recebendo e manipulando os dados. A previsão é de que em 2004, o número de dispositivos sem fio ultrapassará o de computadores pessoais ao acesso à Internet, principalmente com a adoção em massa pelo mercado corporativo (MOURA, 2001).

2.4. SEGURANÇA EM REDES MÓVEIS

Manter o sigilo dos dados é uma questão importante para qualquer rede sem fio. Na época em que a comunicação se restringia à voz, a principal preocupação era a de que intrusos conseguissem ouvir conversas sigilosas. Com o crescimento do sistema móvel, a preocupação com a segurança das informações que trafegam na rede está cada vez maior. Nos dias atuais, muitas empresas ainda têm seus sistemas invadidos, mesmo protegidas por *firewalls*[8], chaves secretas e políticas de segurança. É por este motivo que é necessária a utilização de protocolos criptográficos, que devem ser projetados com a finalidade de fornecerem serviços de segurança como os descritos na TAB. 2.2.

TAB. 2.2 – Serviços de segurança

Serviços de Segurança	Descrição
Estabelecimento da chave de sessão	Durante o processo de autenticação, um segredo comum (chave de sessão) deve ser negociado entre as partes envolvidas na comunicação. Esta chave pode ser usada repetidamente em algumas situações, mas devido aos problemas de segurança, é recomendado o uso de uma nova chave para cada sessão.
Sigilo das mensagens	Uma mensagem transmitida depois de uma inicialização de chamada, incluindo voz e dados, deve ser protegida de intrusos. Isto é conseguido pelo ciframento da mensagem com a chave de sessão secreta estabelecida entre os participantes da comunicação durante o processo de autenticação.
Sigilo da identidade de quem está chamando	Como a identidade do assinante, ou a sua localização, podem ser de especial interesse a algumas pessoas, não devem ficar expostas. Por exemplo, num ambiente militar, é imprescindível esconder a sua localização do inimigo.
Autenticação mútua	Para que um intruso não se passe por uma entidade legítima, é importante que as partes envolvidas na comunicação autentiquem-se, mutuamente.
Não-repúdio do serviço	O uso fraudulento dos serviços de comunicação sem fio é um dos maiores problemas, afinal, não existe associação física entre as entidades. Deve-se assegurar que o emissor de uma mensagem não negue posteriormente o que foi emitido ou até mesmo a sua participação em uma transação.

[8] *Firewalls* – barreiras de proteção (SOARES, LEMOS e COLCHER, 1995)

Além dos serviços de segurança, mostrados na TAB. 2.2, devem ser observadas algumas características do ambiente móvel, no planejamento dos protocolos, tais como:

- requerimentos computacionais: um ambiente sem fio, normalmente, requer dispositivos de baixa potência computacional, implicando que o número e a complexidade das operações de ciframento sejam mantidas tão baixa quanto possível (BASYOUNI e TAVARES, 1996);
- número de mensagens trocadas: por causa do atraso no canal de comunicação, um número grande de mensagens poderá implicar na espera do usuário, desde o momento que ele solicitou uma chamada, até a chamada ser iniciada (RAMASAMI, 2000). Por este motivo, no desenvolvimento de protocolos de segurança para o ambiente de comunicação móvel sem fio, exige-se que o número de mensagens seja reduzido;
- carga computacional da unidade móvel: é importante ter uma carga computacional baixa, pois uma baixa potência consumida pela estação móvel implica num baixo consumo de bateria;
- requerimentos de armazenamento: inclui o espaço requerido para guardar as chaves (pública ou privada), os certificados, ou qualquer dado extra requerido pelo protocolo. É desejável ter baixos requerimentos de armazenamento na estação móvel.

Existem ainda outros fatores que podem ser levados em conta durante o planejamento:

- necessidade de uma Autoridade Central (AC): em alguns protocolos existe a FIG. de uma terceira parte confiável globalmente, responsável pela manutenção da base de dados e pela emissão das chaves e dos certificados;
- função da Autoridade Central (AC): a AC pode ser passiva ou ativa. Uma AC passiva trabalha somente durante o processo de inicialização, ou seja, tem a função de registrar usuários e emitir certificados, enquanto que uma AC ativa participa na execução do protocolo, geralmente causando um grande número de

mensagens a serem transferidas no canal de comunicação (PATIYOOT e SHEPHERD,1998);

- uso de *timestamps*: *timestamps* certificam que os dados existentes estão sendo usados num certo tempo ou data. São usados para evitar os problemas de segurança, como o não-repúdio ou o ataque por repetição, mas possui como problema a sincronização dos relógios das máquinas das entidades (RUBIN e HONEYMAN, 1993);
- uso de *nonces*: *nonces*[9] são identificadores únicos colocados nas mensagens. Em alguns protocolos, os números aleatórios são considerados como identificadores. Eles evitam alguns dos problemas encontrados com o uso dos *timestamps*, tal como a necessidade de sincronização das máquinas. Porém, os identificadores, precisam ser memorizados para sempre. Uma falha em uma das máquinas e a perda da lista de identificadores, deixa a rede vulnerável ao ataque por repetição. Os *timestamps* e os identificadores podem ser combinados, limitando o tempo em que eles devem ser memorizados (TANENBAUM, 1996);

2.5. MÉTODOS FORMAIS

Assume-se que a rede é um ambiente hostil, onde pode haver intrusos que podem ler, modificar e apagar os dados que trafegam nela e ter o controle sobre um ou mais integrantes. Por isso, se o protocolo criptográfico não for projetado cuidadosamente, poderá conter falhas ficando sujeitos a ataques que não são facilmente detectados. Por exemplo, o protocolo de chave-pública de Needham-Schroeder usado na comunicação entre participantes e que era considerado seguro, está sujeito ao ataque do homem-no-meio quando um dos participantes é considerado desonesto (DENNING e SACCO, 1981).

O exemplo acima mostra que o planejamento informal de protocolos criptográficos está propenso a erros. Os métodos formais podem ajudar a resolver esse problema. Eles têm sido empregados no planejamento e na análise de protocolos criptográficos em geral, principalmente os de autenticação e distribuição

[9] Os *nonces*, no restante deste trabalho, serão chamados de identificadores.

de chaves. As técnicas formais podem ser utilizadas em várias fases do projeto de protocolos, incluindo a especificação, a construção e a verificação.

A maioria dos trabalhos desenvolvidos concentram-se na verificação e na especificação formal de protocolos, porém, seria mais barato empregar estes métodos no planejamento do protocolo logo no início, economizando, dessa forma, com as despesas de manutenção posteriores. Além disso, a utilização de métodos formais para o planejamento de protocolos continua sendo uma área pouco explorada (BUTTYÁN, 1999).

Os métodos formais permitem fazer uma análise completa dos diferentes modos de ataque de um intruso e concluir se os objetivos de segurança proposto pelo protocolo foram alcançados. Existem quatro abordagens diferentes para a análise de protocolos criptográficos (FREIRE, 2000), (MEADOWS, 1995), (GRITZALIS, SPINELLIS e GEORGIADIS, 1999) e (RUBIN e HONEYMAN, 1993). A primeira abordagem é a menos popular, enquanto que a terceira é a mais utilizada:

1. modelando e verificando os protocolos usando linguagens de especificação e ferramentas de verificação para a análise de protocolos criptográficos;
2. desenvolvendo sistemas especialistas que um projetista de protocolos pode usar para investigar diferentes cenários;
3. modelando e verificando o protocolo empregando modelos baseados em lógicas modais que analisam a evolução dos conceitos de crença e de conhecimento aplicados aos participantes do protocolo criptográfico ao longo da execução do mesmo. São os métodos mais utilizados na análise de protocolos de autenticação e distribuição de chaves;
4. desenvolvendo um modelo formal baseado em sistemas algébricos que reescrevem as propriedades dos protocolos criptográficos. São complementares aos métodos de lógica modal, pois também são baseados na formalização de problemas por hipóteses e nas propriedades de autenticação.

2.5.1. MÉTODOS BASEADOS EM LINGUAGENS DE VERIFICAÇÃO

Este método analisa o protocolo criptográfico empregando linguagens de especificação e ferramentas de verificação não desenvolvidas especificamente para a análise do protocolo. O objetivo principal desta abordagem é tratar o protocolo criptográfico como qualquer outro programa e tentar provar sua corretude.

O primeiro passo é aplicar técnicas para especificar o protocolo e seus requerimentos de corretude. Em (RUBIN e HONEYMAN, 1993) é realizado um resumo sobre tais métodos. Dentre eles, podem ser destacados:

- LOTOS (*Language of Temporal Ordering Specification*) empregada na especificação de protocolos de autenticação. Em (VARADHARAJAN, 1990) é utilizada LOTOS para analisar alguns protocolos, o problema é que ela não conseguiu demonstrar qualquer resultado. O artigo (VARADHARAJAN, 1990) concluiu que essa ferramenta não é adequada para este tipo de análise;
- *Ina Jo* é uma linguagem de especificação formal que gera teoremas que podem ser usados para verificar se os objetivos do protocolo foram satisfeitos. No artigo (KEMMERER, 1989) é mostrada uma fraqueza nesse sistema;
- Diagrama de Estados é usado em (VARADHARAJAN, 1989) para descrever cada fase de um protocolo. Dessa forma, o projetista pode investigar várias execuções do protocolo aplicando técnicas de análise que são efetivas para determinar se o protocolo está ou não correto, mas eles não garantem a resistência contra um intruso ativo;
- CSP (*Communicating Sequential Processes*) e FDR (*Failure Divergence's Refinement*) – modela os participantes do protocolo como um CSP e usa o verificador FDR. O FDR é empregado para analisar muitos sistemas, incluindo bases de dados, protocolos de comunicação e protocolos de segurança. Outra abordagem é utilizar o HOL (*Higher Order Logic*) para declarar e provar propriedades dos protocolos criptográficos;

Apesar das tentativas em utilizar os métodos baseados em linguagens de especificação na análise de protocolos criptográficos, em geral, eles não são

desenvolvidos para este propósito. A principal crítica destas abordagens é que eles provam a corretude, mas não a segurança.

2.5.2. MÉTODOS BASEADOS EM CENÁRIOS (SISTEMAS ESPECIALISTAS)

A idéia principal desta abordagem é desenvolver sistemas especialistas que podem gerar e investigar vários cenários no protocolo criptográfico. A maioria destes sistemas modelam o protocolo como uma máquina de estados. Estes sistemas iniciam com um estado inseguro e tentam descobrir um caminho para este estado, partindo do estado inicial (BUTTYÁN, 1999). Os principais são:

- *Interrogator*: é o primeiro sistema que utiliza esta abordagem. Os participantes do protocolo na comunicação são modelados como máquinas de estados. As mensagens trocadas entre eles são interceptadas por um intruso que pode apagá-las, modificá-las etc. Os participantes tentam localizar falhas de segurança através de pesquisas exaustivas do estado. O *Interrogator* não encontrou nenhum ataque desconhecido de um protocolo criptográfico, mas tem sido capaz de reproduzir ataques conhecidos;
- Analisador de protocolos NRL (*Navy Research Laboratory's Protocol Analyzer*) é similar ao *Interrogator*: o projetista especifica um estado inseguro e o analisador tenta construir um caminho para esse estado partindo de um estado inicial. Ao contrário do *Interrogator*, um número ilimitado de execuções do protocolo são permitidas num único caminho. Isto permite que o analisador descubra ataques onde um intruso seja capaz de abrir várias sessões diferentes do protocolo ao mesmo tempo. O NRL consegue gerar ataques para protocolos inseguros e provas de segurança para protocolos seguros. Mesmo solicitando alguma intervenção humana, o NRL encontrou falhas em protocolos criptográficos que não foram encontradas utilizando outros analisadores de máquinas de estados.

Os sistemas especialistas são desenvolvidos especificamente para a análise de protocolos criptográficos e obtiveram mais êxito do que os métodos mostrados na

seção anterior, porém, possuem como desvantagem a grande quantidade de possíveis eventos que devem ser examinados.

2.5.3. MÉTODOS BASEADOS EM LÓGICAS MODAIS

Os sistemas baseados em lógica modal consistem em várias declarações de crença ou de conhecimento sobre as mensagens em sistemas distribuídos, com regras para derivar crenças de outras crenças e conhecimentos de outros conhecimentos e crenças (SYVERSON e CERVESATO, 2000).

Estes métodos tornaram-se mais populares e mais utilizados depois do desenvolvimento da lógica formal para a análise do conhecimento e crença, chamada lógica BAN (BURROWS, ABADI e NEEDHAM, 1990). A lógica BAN é a mais utilizada para analisar protocolos de autenticação. Ela não fornece prova de segurança, somente argumenta sobre a autenticação, também não tenta fazer a distinção entre receber uma mensagem e possuí-la; ambas são tratadas do mesmo modo. Os desenvolvedores da lógica BAN tinham como meta responder as seguintes perguntas:

- Quais são os objetivos do protocolo?
- O protocolo precisa de mais suposições do que um outro?
- O protocolo leva em consideração passos desnecessários que poderiam ser omitidos sem prejudicá-lo?
- O protocolo cifra uma mensagem que poderia ser enviada em texto em claro sem prejudicar os aspectos de segurança?

Existem três estágios principais para analisar o protocolo usando a lógica BAN. O primeiro passo é expressar as suposições e os objetivos como declarações (afirmações) numa notação simbólica para que a lógica passe de um estado conhecido para um onde possa certificar se as metas serão realmente alcançadas. Depois é transformar os passos do protocolo numa notação simbólica. Finalmente, um conjunto de postulados são aplicados para atingir os objetivos de autenticação.

Apesar das críticas, a lógica BAN tem sido utilizada com êxito. Ela encontrou falhas em vários protocolos, incluindo o de Needham-Schroeder e no *draft* CCITT X.509 – onde mostrou que um intruso pode utilizar uma chave de sessão antiga e ser aceito, estando ou não a chave comprometida. Descobriu redundâncias em outros protocolos, como o de Yahalom, Needham-Schroeder e Kerberos. Além disso, muitos artigos publicados usam a lógica BAN para legitimar a segurança de seus protocolos, incluindo o de Diffie-Hellman (AZIZ e DIFFIE, 1994) que propôs um protocolo de autenticação para o ambiente de comunicação móvel.

Embora muitas variações e extensões tenham sido propostas, a maioria dos projetistas ainda fazem referência ao trabalho original da lógica BAN. O de maior sucesso entre eles é a GNY, desenvolvida por Gong, Needham e Yahalom (GONG, NEEDHAM e YAHALOM, 1990). A lógica GNY analisa o protocolo passo a passo e torna explícita qualquer suposição necessária. Ela oferece algumas vantagens sobre a lógica BAN, pois fornece forte ênfase na separação entre o conteúdo e o significado das mensagens e é capaz de analisar em mais níveis, já que possui uma quantidade maior de regras. Na lógica GNY, os participantes podem incluir dados nas mensagens para testar o protocolo.

Infelizmente, a lógica GNY é muito mais complexa do que os outros métodos baseados em lógica modal, possui muitas regras que devem ser consideradas em cada fase e, por isso, acredita-se, por alguns autores, não ser prática (GRITZALIS, SPINELLIS e GEORGIADIS, 1999) e (MEADOWS, 1995).

Estas abordagens são as mais empregadas na análise de protocolos criptográficos, provavelmente, porque são mais simples e intuitivas. Porém, o projetista deve ter cuidado, pois algumas suposições podem conduzir a erros na análise.

2.5.4. MÉTODOS BASEADOS EM SISTEMAS ALGÉBRICOS

Esta abordagem é a mais nova dos três métodos para a análise de protocolos criptográficos, porém existem poucas pesquisas nesta área comparadas aos métodos baseados em sistemas modais. Nesta abordagem, o protocolo é modelado

como um sistema algébrico, associando um estado como o conhecimento dos participantes do protocolo. Como os objetos modelados correspondem fortemente às entidades e às mensagens utilizadas nas ferramentas baseadas em máquinas de estado, sugere-se que os modelos algébricos podem ser usados para fornecer ferramentas de máquinas de estado com uma capacidade maior de modelar o conhecimento de um intruso.

O primeiro trabalho nesta área é o sistema de Dolev-Yao (RUBIN e HONEYMAN, 1993) e (MEADOWS, 1995). Nesse modelo assume-se que a rede está sob o controle de um intruso que pode ler, alterar, apagar as mensagens, além de executar qualquer operação, como por exemplo o ciframento das informações. Porém, assume-se inicialmente, que o intruso não conhece qualquer informação que está mantida em segredo, como as chaves que pertencem aos usuários legítimos do sistema.

Como o intruso pode impedir que uma mensagem chegue ao seu destino, o sistema de Dolev e Yao trata qualquer mensagem enviada ou recebida de um usuário legítimo como uma mensagem enviada ou recebida de um intruso. Assim, o sistema vira uma máquina de gerar palavras que pode ser usada pelo intruso. Estas palavras obedecem certas regras de reescrita, como por exemplo: as operações de ciframento e deciframento com a mesma chave cancelam-se uma a outra. Dessa forma, o intruso manipula um termo reescrevendo o sistema.

O modelo de Dolev e Yao tem restrições para a análise da maioria dos protocolos, pois somente pode ser empregado na detecção de falhas de segredo e não permite que os participantes se lembrem das informações de um estado anterior ao seguinte. Os outros trabalhos desenvolvidos nesta área são versões estendidas do modelo de Dolev e Yao.

2.6. CONSIDERAÇÕES FINAIS

Neste capítulo foi apresentada uma revisão bibliográfica dos conceitos básicos de segurança, do ambiente de comunicação móvel celular e dos métodos formais

para a análise de protocolos criptográficos. Estes conceitos serão úteis no entendimento dos capítulos restantes.

No terceiro capítulo serão descritas mais detalhadamente as lógicas BAN e GNY. Além da comparação entre os dois métodos, utilizando como base a análise do protocolo de distribuição de chaves Needham-Schroeder.

3. COMPARAÇÃO ENTRE AS LÓGICAS BAN E GNY

3.1. INTRODUÇÃO

Protocolos criptográficos são pequenas seqüências de mensagens trocadas entre os integrantes[10] de uma rede, geralmente envolvendo ciframento, com o propósito de estabelecer comunicações seguras na rede (BRACKIN, 1999).

Os protocolos criptográficos são utilizados para implementação de serviços de segurança tais como sigilo, integridade, autenticação e não repúdio. No entanto, os protocolos estão sujeitos a erros no desenvolvimento. Uma análise de requisitos do protocolo criptográfico que não capture os reais requisitos do usuário, ou uma falha no projeto, ou uma falha na análise e na verificação de conformidade com os requisitos poderá levar ao desenvolvimento e implementação de um protocolo criptográfico que não garantirá os serviços de segurança desejados pelo usuário (FREIRE, 2000).

Mesmo que um protocolo seja desenvolvido de forma correta, não existirá a garantia de que ele realizará os serviços de segurança para o qual foi desenvolvido. Isso porque, na utilização de um protocolo criptográfico deve ser levada em conta a ação de agentes externos.

Tais agentes externos são chamados de invasores ou intrusos e são participantes da rede de computadores que tentam subverter os objetivos do protocolo criptográfico a fim de impossibilitar a realização dos serviços de segurança pelos quais ele é responsável. Esses intrusos podem atacar os protocolos criptográficos das seguintes formas: pela substituição, modificação, exclusão ou criação de mensagens, ou pelo ataque aos algoritmos criptográficos utilizados.

O desenvolvimento de protocolos criptográficos é, portanto, bastante complexo e não é incomum que sejam descobertas falhas em protocolos que já estejam sendo utilizados e estudados por vários anos. Como exemplo, pode-se citar o protocolo

[10] No restante deste trabalho, integrantes de uma rede serão chamados de participantes, e podem ser usuários finais, entidades, processos ou sistemas de computadores.

para distribuição de chaves Needham-Schroeder (NEEDHAM e SCHROEDER, 1978), utilizado durante quatro anos, até que os pesquisadores D. Denning e G. Sacco demonstraram que ele possuía uma falha e propuseram um protocolo criptográfico alternativo (DENNING e SACCO, 1981). Porém, em 1994, Abadi e Needham demonstraram que este protocolo também possuía uma falha (SYVERSON e CERVESATO, 2000). Em (LOWE, 1995) é apresentado um ataque, até então desconhecido, a outro dos protocolos do trabalho original de Needham-Schroeder, 17 anos depois de sua publicação. Geralmente, quando são descobertas falhas no protocolo criptográfico, elas são corrigidas e adotadas abordagens para evitar o seu uso.

Durante a última década, vários métodos formais têm sido propostos a fim de analisar e projetar protocolos criptográficos (MEADOWS, 2000) e (GRITZALIS, SPINELLIS e GEORGIADIS, 1999). Embora muitos desses trabalhos possam ser aplicados aos protocolos criptográficos, de uma forma geral, a maioria foram elaborados para os protocolos de autenticação e distribuição de chaves.

Os métodos formais podem ser úteis para analisar a segurança de protocolos criptográficos. Eles permitem fazer uma análise completa dos diferentes caminhos que um intruso pode tomar e especificar se os objetivos propostos pelos autores do protocolo foram alcançados. Para a utilização de tais métodos, os protocolos criptográficos devem ser traduzidos da notação não-formal encontrada na literatura para uma notação formal. Assim, algumas linguagens formais de especificação de protocolos criptográficos foram propostas (MEADOWS, 1995) e (BUTTYÁN, 1999) e vêm sendo usadas na análise dos mesmos.

Este trabalho tem como finalidade mostrar a necessidade da análise formal por parte dos projetistas de protocolos criptográficos. Neste capítulo foi realizado um estudo entre as duas lógicas mais conhecidas e utilizadas, denominadas de lógica BAN e lógica GNY e feita uma comparação entre elas. Para isso é feita a análise formal detalhada do protocolo de distribuição de chaves Needham-Schroeder onde são apontadas as principais diferenças entre as duas lógicas e se o objetivo proposto pelos autores do protocolo, ou seja, a distribuição de chaves, foi satisfeito.

O capítulo está organizado da seguinte forma: na seção 3.2 é mostrado o protocolo para distribuição de chaves Needham-Schroeder. Na seção 3.3 é mostrada uma descrição das lógicas BAN e GNY, da notação básica, dos símbolos

e dos postulados lógicos utilizados. Na seção 3.4 é realizada uma comparação entre as duas abordagens e são feitas as considerações finais do capítulo.

3.2. PROTOCOLO PARA DISTRIBUIÇÃO DE CHAVES NEEDHAM-SCHROEDER

Antes de realizar a descrição das lógicas será necessário mostrar o funcionamento do protocolo para distribuição de chaves Needham-Schroeder (NEEDHAM e SCHROEDER, 1978). Este protocolo foi escolhido, pois influenciou no desenvolvimento de outros sistemas existentes e publicados e também, porque serve como exemplo para a análise da maioria dos métodos já que possui falhas conhecidas.

O protocolo de Needham-Schroeder usa um mecanismo denominado desafio-resposta e foi utilizado durante anos, até que, em 1981 os pesquisadores D. Denning e G. Sacco (*Timestamps in Key Distribution Protocols*) demonstraram que ele possuía uma falha e propuseram um protocolo criptográfico alternativo (FREIRE, 2000).

O objetivo geral deste protocolo é fornecer uma chave de sessão compartilhada entre dois participantes (A e B). Existe uma autoridade central (S) confiada globalmente pelos participantes e que compartilha uma chave secreta com cada um deles (ex. A compartilha a chave secreta K_{as} com S e B compartilha a chave secreta K_{bs} com S). S também tem a responsabilidade de gerar as chaves de sessão, que serão utilizadas entre os participantes para o ciframento das mensagens durante a comunicação (ver FIG. 3.1).

- Fluxo de Mensagens

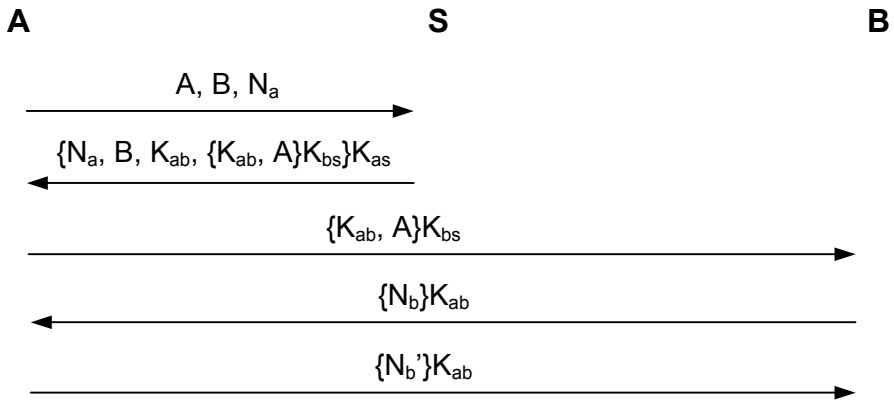

FIG. 3.1 – Protocolo de Distribuição de Chaves Needham-Schroeder

O protocolo Needham-Schroeder consiste em cinco mensagens:

Mensagem 1	A → S:	A, B, N_a
Mensagem 2	S → A:	{N_a, B, K_{ab}, {K_{ab}, A}K_{bs}}K_{as} ⇨ {N_a, B, K_{ab}, F}K_{as}
Mensagem 3	A → B:	{K_{ab}, A}K_{bs}
Mensagem 4	B → A:	{N_b}K_{ab}
Mensagem 5	A → B:	{N_b'}K_{ab}

N_a = identificador gerado por A;
N_b = identificador gerado por B;
K_{as} = chave secreta compartilhada entre A e S;
K_{bs} = chave secreta compartilhada entre B e S;
K_{ab} = chave de sessão gerada pela autoridade central S e enviada para os participantes (A e B).

1º passo: A envia sua identidade, a identidade do participante que ele quer se comunicar (B) e um identificador (N_a) gerado por ele, para a autoridade central S;
2º passo: S gera uma chave de sessão (K_{ab}) e duas mensagens: uma contendo a chave de sessão e a identidade de A, tudo isto cifrado com a chave secreta (K_{bs}) que B compartilha com S (função F); a outra mensagem contém o identificador gerado por A (enviado na primeira mensagem), a identidade de B, a chave de

sessão e a função F, tudo cifrado com a chave secreta que A compartilha com S (K_{as}). Esta mensagem é enviada para A;

3º passo: A decifra a mensagem utilizando sua chave secreta (K_{as}) obtém a chave de sessão (K_{ab}) e verifica o identificador. Se o valor do identificador for o esperado, então A repassa a mensagem que está cifrada com a chave secreta que ele não possui (K_{bs}) para B.

4º passo: B decifra a mensagem utilizando a chave secreta compartilhada entre ele e S, verifica qual o participante que quer se comunicar com ele e obtém a chave de sessão (K_{ab}). Depois gera um novo identificador (N_b), cifra-o com a chave de sessão recebida e o envia para A;

5º passo: A recebe a mensagem, decifra-a usando a chave de sessão e obtém o identificador gerado por B. Depois, envia uma mensagem para B contendo o identificador (N_b') cifrado com a chave de sessão (K_{ab}).

Depois de executados estes passos, o protocolo terá conseguido realizar de forma segura a distribuição da chave de sessão, que será utilizada entre os participantes A e B para o ciframento das mensagens transmitidas na comunicação.

Na seção seguinte, o protocolo mostrado na FIG. 3.1 será analisado pelas lógicas BAN e GNY, e para isto, será traduzido para uma notação idealizada.

3.3. DESCRIÇÃO DOS MÉTODOS

3.3.1. LÓGICA BAN

A lógica BAN foi desenvolvida por Burrows, Abadi e Needham (por isso o nome) em 1989 (versão original) e foi a primeira a analisar formalmente os protocolos criptográficos (KYNTAJA, 1995). É a lógica mais popular na literatura para a análise dos protocolos, principalmente os de autenticação e de distribuição de chaves. Em (BURROWS, ABADI e NEEDHAM, 1990) são apresentadas a notação e os postulados lógicos, e é realizada a análise formal (utilizando a lógica BAN) de vários

protocolos criptográficos, tais como: Otway-Rees, Kerberos, Wide-mouthed Frog, Andrew Secure RPC Handshake e o CCITT X.509.

A lógica não fornece uma prova de segurança; pode somente argumentar sobre a autenticação, porém, é uma lógica simples, direta, fácil de aplicar e ainda é útil na detecção de falhas. Os criadores da lógica BAN, descrevem a proposta da lógica da seguinte maneira:

"O objetivo da lógica é descrever a crença das partes envolvidas na autenticação e a evolução desta crença enquanto os participantes se comunicam" (BURROWS, ABADI e NEEDHAM, 1990).

Por exemplo, se uma regra diz que A acredita que a chave K só é conhecida por ele e por B, e A recebe uma mensagem cifrada com K, então A acredita que a mensagem foi enviada de B para A ou de A para B.

Para utilizar essa abordagem, o método convencional de descrever os protocolos que lista a origem, o destino e o conteúdo, é substituído por fórmulas que permitem representar os passos do protocolo de forma que todas as informações essenciais sejam mostradas. Isto é denominado de protocolo idealizado. Além disso, são realizadas afirmações com o protocolo idealizado, descrevendo as crenças dos participantes. O protocolo é analisado passo a passo com um conjunto de regras até se chegar em algum dos objetivos de autenticação (dependendo das metas dos protocolos) mostrados a seguir:

- A acredita $A \leftrightarrow^{k} B$ (ex: A acredita que A e B compartilham a chave k)
- B acredita $A \leftrightarrow^{k} B$
- A acredita B acredita $A \leftrightarrow^{k} B$
- B acredita A acredita $A \leftrightarrow^{k} B$

Na lógica BAN a análise de um protocolo é dividida em quatro fases:

1. o protocolo idealizado é derivado da notação original;
2. as suposições são escritas de acordo com o estado inicial do protocolo;

3. as declarações do protocolo e as afirmações sobre o estado do sistema são anexadas às fórmulas lógicas;
4. os postulados lógicos são aplicados nas suposições e nas afirmações para descobrir as crenças dos participantes no protocolo.

Basicamente, as suposições incluem as declarações sobre a posse e a distribuição das chaves, a criação de identificadores e a crença entre os participantes.

A lógica BAN consiste em regras muito simples, intuitivas e é possível usá-la para encontrar falhas graves em protocolos bastante conhecidos e utilizados, como os citados anteriormente. Como resultado, a lógica ganhou muita atenção e outras lógicas começaram a ser desenvolvidas estendendo ou aplicando o mesmo conceito de crença para diferentes tipos de problemas em protocolos criptográficos (SYVERSON e CERVESATO, 2000).

3.3.1.1. NOTAÇÃO BÁSICA

A lógica contém três tipos de objetos: participantes, chaves de ciframento e fórmula[11] (também chamada de declaração). As mensagens são identificadas como declarações na lógica. As letras A, B e S denotam, tipicamente, as entidades, sendo A e B os participantes que pretendem trocar informações entre si e S a autoridade central; o K_{ab}, K_{as} e K_{bs} são as chaves secretas compartilhadas entre os participantes; K_a, K_b e K_s são as chaves públicas; K_a^{-1}, K_b^{-1} e K_s^{-1} são as chaves privadas correspondentes de cada participante; e N_a, N_b e N_s são os identificadores gerados pelos participantes.

Além dos objetos mencionados acima, a lógica BAN utiliza uma notação básica, mostrada a seguir, na transformação do protocolo convencional para o protocolo idealizado e na análise do mesmo:

---

[11] Neste trabalho, fórmula será o nome usado para fazer referência a uma *string*, que possui um determinado valor, durante a execução do protocolo. Como exemplo de fórmulas podem ser citadas as variáveis X e Y.

1. P $\models$ X: P acredita em X, ou P está autorizado a acreditar em X. P pode agir como se X fosse verdadeiro. Esta é a declaração central da lógica;
2. P $\lhd$ X: P recebe X. P recebeu uma mensagem contendo X, e por isso, P pode obter X da mensagem. P pode ler e repetir X (possivelmente depois de algum deciframento);
3. P $\mid\sim$ X: P disse X. O participante P enviou uma mensagem contendo a declaração X em algum momento. Nenhuma conclusão imediata pode ser feita, a não ser que a mensagem tenha sido enviada há algum tempo ou durante a execução atual do protocolo. Sabe-se que P acreditou em X quando a mensagem foi enviada;
4. P $\Rightarrow$ X: P tem jurisdição sobre X. O participante P é uma autoridade sobre X e deve ser confiado nesta importância. Esta declaração é usada quando uma entidade é responsável, por exemplo, pela criação da chave de sessão;
5. #(X): A fórmula X é nova, ou seja, ela não foi utilizada antes numa outra sessão do protocolo. Os identificadores e os *timestamps* são comumente gerados com a finalidade de serem novos;
6. P $\overset{k}{\leftrightarrow}$ Q: P e Q podem usar a chave compartilhada k para se comunicarem. A chave k é considerada satisfatória já que nunca será descoberta por qualquer participante, exceto P ou Q, ou por alguém em quem eles confiam;
7. $\overset{k}{\mapsto}$ P: P possui como chave pública k. A correspondente chave privada k^{-1} é conhecida somente por P ou pelo participante em quem ele confia;
8. P $\overset{X}{\rightleftharpoons}$ Q: A fórmula X é um segredo conhecido somente por P e Q e, possivelmente, pelo participante em quem eles confiam. X pode ser utilizado somente por P ou Q para provar suas identidades. X é tão novo quanto secreto. Uma senha é um exemplo de um segredo compartilhado;
9. {X}k: representa que a fórmula X foi cifrada com a chave k;
10. <X>Y: representa a combinação da fórmula X com a fórmula Y. Esta representação só é utilizada quando o segredo é solicitado como uma prova de identidade.

3.3.1.2. POSTULADOS LÓGICOS

Em qualquer estudo dos protocolos de segurança é importante distinguir o tempo das demonstrações ou eventos. Caso contrário, o reenvio de mensagens anteriores poderá ocorrer sem serem descobertas. A lógica BAN divide o tempo em duas épocas: passado e presente. Considera-se como presente o tempo durante a execução atual do protocolo. Qualquer mensagem enviada antes disto é considerada do passado e deve ser rejeitada pelo protocolo como não confiável. Para a lógica, esta simples divisão de tempo é suficiente para analisar os protocolos de autenticação.

Um importante fator em qualquer protocolo de segurança é o ciframento das mensagens. Embora a lógica BAN não tente fazer a avaliação da força do sistema criptográfico que está sendo usado, ela faz certas suposições relativas ao processo de ciframento:

1. o ciframento garante que cada seção cifrada não pode ser alterada ou dividida em seções menores. Se uma mensagem contiver duas seções de ciframento separadas, elas serão tratadas como se tivessem chegado de mensagens separadas;
2. uma mensagem não pode ser compreendida por um participante que não conheça a chave secreta (ou a chave privada no caso do sistema criptográfico de chave pública);
3. as mensagens precisam conter informações suficientes para um participante detectar (e ignorar) suas próprias mensagens.

A seguir, está a lista dos postulados usados na lógica BAN para a realização da análise dos protocolos de segurança (BURROWS, ABADI e NEEDHAM, 1990).

B1. REGRA DO SIGNIFICADO DA MENSAGEM (*Message-meaning rule*): esta regra faz parte da interpretação das mensagens. Pode ser aplicada de três formas diferentes chegando ao mesmo resultado. As duas primeiras para as mensagens cifradas: usando chaves secretas compartilhadas (B1.1) ou utilizando chaves públicas (B1.2) e a última (B1.3) para as mensagens com segredos.

B1.1. Para as chaves secretas compartilhadas:

$$\frac{P \models Q \overset{k}{\leftrightarrow} P,\ P \triangleleft \{X\}K}{P \models Q \mid\sim X}$$

Se Q e P compartilham uma chave secreta K e P recebe uma mensagem cifrada usando K, então ele acredita que Q, em algum momento, disse X.

B1.2. Para as chaves públicas:

$$\frac{P \models \overset{k}{\mapsto} Q,\ P \triangleleft \{X\}\ K^{-1}}{P \models Q \mid\sim X}$$

B1.3. Para segredos compartilhados:

$$\frac{P \models Q \overset{Y}{\rightleftharpoons} P,\ P \triangleleft \langle X \rangle Y}{P \models Q \mid\sim X}$$

Se P e Q compartilham um segredo Y e P recebe X com o segredo compartilhado Y, então P acredita que Q, em algum momento, disse X.

B2. REGRA DE VERIFICAÇÃO DO IDENTIFICADOR (*Nonce-verification rule*): verifica se a mensagem é recente (ou seja, se foi enviada durante a execução atual do protocolo) e conseqüentemente, se o emissor acredita nela.

$$\frac{P \models \#(X),\ P \models Q \mid\sim X}{P \models Q \models X}$$

Se P acredita que X é novo e P acredita que em algum momento Q disse X, então P acredita que Q acredita em X.

B3. REGRA DA JURISDIÇÃO (*Juridiction rule*): esta regra representa a confiança e a autoridade de uma entidade sobre as declarações:

$$\frac{P \models Q \Rightarrow X,\ P \models Q \models X}{P \models X}$$

Se P acredita que Q tem jurisdição sobre a declaração X e P acredita que Q acredita em X, então P confia na veracidade de X.

Uma propriedade do símbolo de crença (⊨) é especificar a confiança de P em relação a um conjunto de demonstrações, se e somente se, P acredita em cada demonstração separadamente. Isto justifica as regras B4:

$$\frac{P \models X,\ P \models Y}{P \models (X,Y)} \qquad \frac{P \models (X,Y)}{P \models X} \qquad \frac{P \models Q \models (X,Y)}{P \models Q \models X}$$

B5. Regras similares a anterior podem ser aplicadas ao símbolo $\sim$ (disse):

$$\frac{P \models Q \sim (X,\ Y)}{P \models Q \sim X}$$

Se $P \models Q \sim X$ e $P \models Q \sim Y$ não quer dizer que $P \models Q \sim (X,Y)$, já que implicaria que as duas partes X e Y foram ditas ao mesmo tempo.

B6. O mesmo acontece com o símbolo $\triangleleft$ (recebe):

$$\frac{P \triangleleft (X,Y)}{P \triangleleft X} \qquad \frac{P \triangleleft \langle X \rangle Y}{P \triangleleft X} \qquad \frac{P \models Q \leftrightarrow^{k} P,\ P \triangleleft \{X\}K}{P \triangleleft X}$$

$$\frac{P \models \mapsto^{k} P,\ P \triangleleft \{X\}K}{P \triangleleft X} \qquad \frac{P \models \mapsto^{k} Q,\ P \triangleleft \{X\}K^{-1}}{P \triangleleft X}$$

Se um participante recebe uma fórmula, então ele vê seus componentes, conhecendo as chaves necessárias:

B7. Se uma parte de uma fórmula é nova então toda a fórmula também deve ser nova:

$$\frac{P \models \#(X)}{P \models \#(X,Y)}$$

B8. A mesma chave é utilizada entre os participantes em ambas as direções:

$$\frac{P \models R \leftrightarrow^{k} R'}{P \models R' \leftrightarrow^{k} R} \qquad \frac{P \models Q \models R \leftrightarrow^{k} R'}{P \models Q \models R' \leftrightarrow^{k} R}$$

Logo, se P acredita que a chave k é compartilhada entre dois participante R e R', então P acredita que a chave k é compartilhada entre R' e R. Esta regra também é utilizada para segredos compartilhados.

Estes são os principais postulados utilizados na construção da análise formal de protocolos criptográficos. A descrição completa e outros postulados são encontrados em (BURROWS, ABADI e NEEDHAM, 1990).

3.3.1.3. ANÁLISE FORMAL

Para mostrar o funcionamento da lógica BAN será apresentada a análise formal do protocolo de distribuição de chaves Needham-Schroeder (seção 3.2). Apesar dele ter sido demonstrado no artigo de (BURROWS, ABADI e NEEDHAM, 1990), este trabalho mostra de forma mais detalhada o emprego das regras em cada mensagem enviada pelos participantes explicando todos os passos do protocolo. O protocolo de Needham-Schroeder foi escolhido, pois é bastante conhecido e serve como exemplo para a maioria dos métodos desenvolvidos.

O primeiro passo é transformar o protocolo numa forma idealizada:

- Protocolo Idealizado

Mensagem 2 $S \rightarrow A: \{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), \#(A \overset{K_{ab}}{\leftrightarrow} B), \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}\}K_{as}$

Mensagem 3 $A \rightarrow B: \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}$

Mensagem 4 $B \rightarrow A: \{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab}$

Mensagem 5 $A \rightarrow B: \{N_b', (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab}$

O protocolo idealizado acima só possui mensagens da forma $\{X_1\}K_1,... \{X_n\}K_n$, onde cada parte cifrada é tratada separadamente. A lógica BAN omite as mensagens em texto em claro, porque elas podem ser forjadas, e conseqüentemente, não contribuiriam na análise do protocolo. É por este motivo que a primeira mensagem não é considerada. O resultado é como se a autoridade central S tivesse agido espontaneamente.

A segunda mensagem consiste em quatro fórmulas: um identificador, a chave de sessão (K_{ab}) que será compartilhada entre os participantes A e B, a afirmação de que esta chave é nova e a chave de sessão cifrada com a chave secreta (K_{bs}). Tudo isso cifrado com a chave secreta compartilhada entre A e S (K_{as}).

Como parte da segunda mensagem está cifrada com a chave secreta que B compartilha com S e como A não tem conhecimento dessa chave, então ele simplesmente repassa este pedaço da mensagem para B (terceira mensagem).

As duas últimas mensagens são realizadas para que B tenha certeza de que está se comunicando com A e por isso, gera um novo identificador (N_b) e envia-o cifrado para A com a chave de sessão (K_{ab}) recebida.

O passo seguinte é especificar as suposições que serão empregadas na análise do protocolo:

- Suposições

(1) $A \models A \overset{K_{as}}{\leftrightarrow} S$

(2) $S \models A \overset{K_{as}}{\leftrightarrow} S$

(3) $S \models A \overset{K_{ab}}{\leftrightarrow} B$

(4) $B \models B \overset{K_{bs}}{\leftrightarrow} S$

(5) $S \models B \overset{K_{bs}}{\leftrightarrow} S$

(6) $A \models (S \Rightarrow A \overset{K_{ab}}{\leftrightarrow} B)$

(7) $B \models (S \Rightarrow A \overset{K_{ab}}{\leftrightarrow} B)$

(8) $A \models (S \Rightarrow \#(A \overset{K_{ab}}{\leftrightarrow} B))$

(9) $A \models \#(N_a)$

(10) $B \models \#(N_b)$

(11) $S \models \#(A \overset{K_{ab}}{\leftrightarrow} B)$

(12) $B \models \#(A \overset{K_{ab}}{\leftrightarrow} B)$

As cinco primeiras suposições descrevem as chaves secretas compartilhadas conhecidas pelos participantes. As suposições da sexta à oitava indicam que os participantes confiam no que a autoridade central (S) pode realizar (neste caso, gerar as novas chaves de sessão). As três últimas suposições indicam a crença dos participantes nos identificadores e nas chaves em serem novos.

A décima segunda suposição é considerada duvidosa: B acredita que a chave (K_{ab}) é nova. Esta suposição teve que ser colocada para dar continuidade à análise formal e chegar ao objetivo proposto e, por isso, o protocolo foi criticado (BURROWS, ABADI e NEEDHAM, 1990).

- Prova

A prova a seguir mostra como estas suposições são necessárias para o protocolo atingir o objetivo proposto.

Na primeira mensagem, o participante A envia uma mensagem em texto em claro contendo um identificador gerado por ele que pode ser visto pela autoridade central (S). Na segunda mensagem, S envia para A o identificador recebido e a nova chave de sessão que será usada entre A e B para cifrar, posteriormente, o conteúdo de suas mensagens.

- Mensagem 2: A recebe toda a fórmula (13)

$A \triangleleft \{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), \#(A \overset{K_{ab}}{\leftrightarrow} B), \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}\}K_{as}$ (13)

$A \models S \mid\sim \{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), \#(A \overset{K_{ab}}{\leftrightarrow} B), \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}\}$ (14) (B1, 13 e 1)

$A \models S \mid\sim \{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), \#(A \overset{K_{ab}}{\leftrightarrow} B)\}$ (15) (B5, 14)

A decifra a fórmula (13) utilizando a chave secreta compartilhada entre ele e S. Já que A conhece N_a, e acredita que o N_a é novo (suposição 9), então A pode aplicar a

regra de significado da mensagem (B1) usando a fórmula (13) e a suposição (1) obtendo a fórmula (14). Depois, aplicando a regra de verificação do identificador (B2) na suposição (9) e na fórmula (15) serão geradas as seguintes fórmulas:

$A \models S \models (A \overset{K_{ab}}{\leftrightarrow} B)$ (16) (B5 (B2, 15 e 9))

$A \models S \models (\#(A \overset{K_{ab}}{\leftrightarrow} B))$ (17) (B5 (B2, 15 e 9)

Pela regra da jurisdição (B3) aplicada nas fórmulas 16 e 17, usando as suposições 6 e 8, respectivamente, tem-se:

$A \models (A \overset{K_{ab}}{\leftrightarrow} B)$ (18) (B3, 6 e 16)

$A \models \#(A \overset{K_{ab}}{\leftrightarrow} B)$ (19) (B3, 8 e 17)

Resultado: A obtém a chave de sessão compartilhada com B.

A segunda mensagem contém uma parte que está cifrada com a chave secreta compartilhada entre B e S (K_{bs}) e como A não possui esta chave, então, ele repassa esta parte da mensagem para B por meio da terceira mensagem.

- Mensagem 3: B recebe a mensagem de A (20)

$B \lhd \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}$ (20)

Através da regra de significado da mensagem (B1) aplicada em (20) e na suposição (4), obtém-se:

$B \models S \mid\sim (A \overset{K_{ab}}{\leftrightarrow} B)$ (21) (B1, 20 e 4)

Ao contrário de A, B não é capaz de continuar a não ser que recorra à suposição duvidosa (12). B não reconhece qualquer elemento novo na mensagem e, por isso, ele não pode saber quando esta mensagem foi gerada. Dessa forma, B

simplesmente assume que a mensagem recebida de S é nova. Considerando esta suposição verdadeira, o restante do protocolo não terá nenhum problema.

Aplicando a regra de verificação de identificador (B3) na suposição (12) e na fórmula (21), obtém-se:

$$B \models A \overset{K_{ab}}{\leftrightarrow} B \qquad (22) \quad \text{(B3, 12 e 21)}$$

Resultado: B acredita ter obtido a chave de sessão (K_{ab}) compartilhada com A.

As duas últimas mensagens (mostradas no fluxo de mensagens do protocolo Needham-Schroeder na seção 3.2) são feitas para convencer os participantes A e B da existência de ambos, ou seja, que eles enviaram mensagens recentemente e que estão de posse da chave de sessão.

- Mensagem 4: B gera um identificador (N_b) e envia-o cifrado com a chave de sessão (K_{ab}) para A.

$$A \triangleleft \{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab} \qquad (23)$$

Aplicando a regra de significado da mensagem (B1) nas fórmulas (18) e (23), obtém-se a fórmula (24). Utilizando a regra de verificação do identificador (B2) nas fórmulas (19) e (24) obtém-se a fórmula (25).

$$A \models B \mid\sim A \overset{K_{ab}}{\leftrightarrow} B \qquad (24) \quad \text{(B1, 18 e 23)}$$

$$A \models B \models A \overset{K_{ab}}{\leftrightarrow} B \qquad (25) \quad \text{(B2, 19 e 24)}$$

Resultado: A acredita que B acredita na chave de sessão K_{ab}.

- Mensagem 5: B recebe a mensagem de A.

$$B \triangleleft \{N_b', (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab} \qquad (26)$$

Aplicando a regra de significado da mensagem (B1) nas fórmulas (22) e (26), obtém-se a fórmula (27). Utilizando a regra de verificação do identificador (B2) na suposição (12) e na fórmula (27) obtém-se a fórmula (28).

$B \models A \mid\sim A \overset{K_{ab}}{\leftrightarrow} B$ (27) (B1, 22 e 26)

$B \models A \models A \overset{K_{ab}}{\leftrightarrow} B$ (28) (B2, 12 e 27)

Resultado: B acredita que A também acredita na chave de sessão K_{ab}.

Observe que considerar o identificador N_b novo, é suficiente para B fazer suas deduções e chegar nas seguintes crenças:

- Conclusão

$A \models A \overset{K_{ab}}{\leftrightarrow} B$ (18)

$B \models A \overset{K_{ab}}{\leftrightarrow} B$ (22)

$A \models B \models A \overset{K_{ab}}{\leftrightarrow} B$ (25)

$B \models A \models A \overset{K_{ab}}{\leftrightarrow} B$ (28)

A conclusão mostra que os participantes A e B acreditam na chave de sessão e além disso, acreditam que o outro também acredita na chave, ou seja, o objetivo do protocolo (distribuição da chave) foi satisfeito.

O problema é que este resultado só foi alcançado, porque B aceitou a chave de sessão como nova (suposição 12). B não pode ter certeza se A é um participante honesto ou se é um intruso.

A chave de sessão comprometida pode causar resultados desastrosos: um intruso tem tempo ilimitado (não são utilizados *timestamps*) para encontrar uma chave de sessão antiga e usá-la como se fosse nova. Existem conseqüências mais drásticas se a chave secreta de A estiver comprometida: um intruso pode usá-la para obter a chave de sessão, e com isso, conversar com outros participantes, podendo ter acesso às informações sigilosas. Além de continuar utilizando estas

chaves de sessão, mesmo que a chave secreta de A seja trocada posteriormente. O problema principal é que B não tem nenhuma interação com a autoridade central S (é possível contornar esse problema iniciando o protocolo com B no lugar de A).

De acordo com a análise, empregando a lógica BAN, chega-se a conclusão que para chegar ao objetivo proposto foi necessário considerar uma suposição duvidosa. Logo, a lógica é eficiente na realização da análise formal, já que tornou explícito o problema descrito acima e mostrou que a partir dessa suposição poderão ocorrer falhas no protocolo.

3.3.2. LÓGICA GNY

A lógica BAN estimulou o interesse na aplicação de lógica para a análise de protocolos criptográficos e por isso, outros métodos foram desenvolvidos a fim de aprimorar seus conceitos (GRITZALIS, SPINELLIS e GEORGIADIS, 1999) (SYVERSON e CERVESATO, 2000). O de maior sucesso entre eles, denomina-se lógica GNY (GONG, NEEDHAM e YAHALOM, 1990) que é uma versão estendida da lógica BAN e por isso foi escolhida para a comparação.

Como na lógica BAN, a lógica GNY permite analisar um protocolo passo a passo e para isso as mensagens devem ser transformadas da notação original para uma notação simbólica, onde as suposições e os postulados são aplicados com a finalidade de atingir o objetivo proposto pelo protocolo criptográfico. Na maioria das vezes, as suposições são padrões e mostram quais são as chaves compartilhadas entre os participantes, quais são os números aleatórios gerados e quais participantes são autoridades e se são confiáveis nesta responsabilidade.

Cada participante, em cada sessão, mantém dois conjuntos: um de crenças, que inclui todas as suas convicções atuais e outro de posses, que inclui todas as fórmulas que ele recebe e todas as fórmulas que ele gera, tais como, os identificadores. Os participantes iniciam uma sessão com determinadas crenças e posses, para que durante a execução do protocolo possam ampliar seus conjuntos. Os postulados lógicos, descritos a seguir (seção 3.3.2.2), também derivam novas crenças e posses das mensagens recebidas.

A lógica GNY faz a distinção entre o que um participante possui e o que ele acredita permitindo tratar separadamente o conteúdo de uma mensagem e as informações que podem ser obtidas dela, de forma que poderão ser considerados diferentes níveis de confiança na análise. Também é incluída a notação "não-originada-aqui" nos componentes das mensagens permitindo o participante detectar mensagens que foram enviadas em sessões anteriores (MATHURIA, NAINI e NICKOLAS, 1994).

O conjunto de notações básicas, descrito na lógica BAN (seção 3.3.1.1), foi ampliado de forma que fossem incorporadas propriedades adicionais ao processo de análise. Por exemplo, as fórmulas cifradas e as fórmulas em texto em claro, que não eram consideradas na lógica BAN, são tratadas da mesma maneira pela GNY.

Nas seções a seguir serão descritas a notação básica, os principais postulados lógicos e realizada a análise formal do protocolo Needham-Schroeder (seção 3.2) para distribuição de chaves. Depois serão feitas comparações entre a lógica GNY e a lógica BAN.

3.3.2.1. NOTAÇÃO BÁSICA

1. P ◁ X: P recebe a fórmula X. P recebe X possivelmente depois de executar algum deciframento. Uma fórmula recebida pode ser a própria mensagem, como também qualquer conteúdo computável da mensagem recebida;
2. P ∋ X: P possui a fórmula X. Isto inclui todas as fórmulas que P tenha enviado, todas as fórmulas que P tenha iniciado a sessão e todas as que ele recebeu durante a execução atual do protocolo;
3. P |~ X: P disse a fórmula X. X pode ser uma mensagem ou um conteúdo calculável da mensagem, ou seja, uma fórmula pode estar implícita na mensagem;
4. P ⊨ #(X): P acredita, ou está autorizado a acreditar, que a fórmula X é nova. X não foi utilizada em nenhum momento da execução atual do protocolo. Por exemplo, os identificadores numa fórmula podem ser considerados novos;

5. $P \models \emptyset(X)$: P acredita, ou está autorizado a acreditar, que pode reconhecer a fórmula X. P pode reconhecer um valor (exemplo, sua própria identificação) ou uma estrutura (exemplo, o formato de um *timestamp*);
6. $P \models P \overset{S}{\leftrightarrow} Q$: P acredita, ou está autorizado a acreditar, que S é um segredo satisfatório para P e Q. Eles podem utilizá-lo para provar suas identidades mutuamente. Também podem usá-lo como uma chave para se comunicarem, ou para derivar uma chave de S. S nunca será descoberto por qualquer participante, exceto por P e Q, ou por um participante em quem eles confiam. Porém, este participante nunca deverá usar S como prova de sua identidade ou como uma chave. Esta notação é simétrica: $Q \overset{S}{\leftrightarrow} P$ ou $P \overset{S}{\leftrightarrow} Q$;
7. $P \models P \overset{+K}{\mapsto} Q$: P acredita, ou está autorizado a acreditar, que $+K$ é a chave pública de Q. O $-K$ é a sua respectiva chave privada e nunca será descoberta por qualquer participante, exceto por Q ou pelo participante em quem Q confia. Porém, este participante não deve usá-la nem como prova de sua identidade e nem para se comunicar com Q.

Além da notação descrita acima, a lógica GNY utiliza um asterisco ($*$) colocado na frente de uma fórmula e significa que o termo seguido dele não foi originado pelo participante que o recebeu, por isso é utilizada a expressão: “não-originada-aqui”. A declaração $P \triangleleft *X$ indica que P recebeu uma fórmula X que não foi dita por ele numa mensagem anterior durante a execução atual do protocolo.

3.3.2.2. POSTULADOS LÓGICOS

Existem sete categorias principais de postulados lógicos. Neste trabalho serão mostrados os principais, mas uma lista completa de todos os postulados e de suas descrições são encontradas em (GONG, NEEDHAM e YAHALOM, 1990). Estes postulados são usados na análise formal, juntamente com as suposições e as mensagens recebidas, para se chegar ao objetivo proposto pelo protocolo.

G1. REGRA DE RECEBIMENTO (*Being-Told Rules*): o primeiro conjunto de regras mostra as fórmulas que um participante recebe. São consideradas também as computações feitas com as fórmulas recebidas (exemplo: deciframento da mensagem).

G1.1. Receber uma fórmula implica receber cada um de seus componentes:

$$\frac{P \lhd (X,Y)}{P \lhd X}$$

G1.2. Receber uma fórmula do tipo "não-originada-aqui" é um caso especial de receber uma fórmula:

$$\frac{P \lhd {}^{*}X}{P \lhd X}$$

G1.3 Se um participante recebe uma fórmula cifrada com uma chave que ele possui, então também é considerado que ele recebeu os conteúdos decifrados daquela fórmula:

$$\frac{P \lhd \{X\}_K,\ P \ni K}{P \lhd X}$$

Se P recebe a fórmula X cifrada com a chave K e P possui a chave K, então P recebe a fórmula X.

G2. REGRA DE POSSE (*Possession Rules*): especifica as fórmulas que um participante é capaz de possuir. Exemplos:

G2.1 Um participante é capaz de possuir qualquer fórmula (ou mensagem) recebida:

$$\frac{P \lhd X}{P \ni X}$$

Se P recebe a fórmula X então P possui a fórmula X.

G2.2. Se um participante possui duas fórmulas então ele é capaz de possuir a combinação das duas fórmulas e a função (F) delas:

$$\frac{P \ni X, P \ni Y}{P \ni (X,Y), P \ni F(X,Y)}$$

G3. REGRA DE RECENTIDADE[12] (*Freshness rules*): especifica que um participante acredita que a fórmula é nova, ou seja, a fórmula nunca foi utilizada numa execução anterior do protocolo.

G3.1. Se P acredita que X é nova, então ele está autorizado a acreditar que qualquer fórmula que contenha X é nova e que uma possível função (F) computável de X é nova. Por conveniência, será utilizado: $P \models \#(X,Y)$ para denotar $P \models \#(X)$ ou $P \models \#(Y)$:

$$\frac{P \models \#(X)}{P \models \#(X,Y), P \models \#(F(X))}$$

G3.2. Se P acredita que a fórmula X é nova e possui a chave (K) então P está autorizado a acreditar que o ciframento (ou o deciframento) de X com a chave K é nova:

$$\frac{P \models \#(X), P \ni K}{P \models \#(\{X\}_K), P \models \#(\{X\}_K^{-1})}$$

G4. REGRA DE RECONHECIMENTO (*Recognizability rules*): especifica que um participante pode acreditar no reconhecimento de uma fórmula, já que acredita no reconhecimento de outras fórmulas.

[12] Recentidade é a qualidade do que é recente (*freshness*) (Dicionário Houaiss, página 2399, ed. Objetiva – 2001).

G4.1. Se P acredita que reconhece a fórmula X, então P está autorizado a acreditar que reconhece qualquer fórmula que contenha X e que reconhece uma possível função (F) de X:

$$\frac{P \models \text{Ø}\ (X)}{P \models \text{Ø}\ (X,Y), P \models \text{Ø}\ (F(X))}$$

G4.2. Se P acredita que reconhece a fórmula X e P possui a chave K, então P está autorizado a acreditar que reconhece o ciframento e/ou o deciframento de X com a chave K:

$$\frac{P \models \text{Ø}\ (X),\ P \ni K}{P \models \text{Ø}\ (\{X\}_K),\ P \models \text{Ø}\ (\{X\}_K^{-1})}$$

G5. REGRA DE INTERPRETAÇÃO DA MENSAGEM (*Message Interpretation Rules*): estas regras permitem aos participantes desenvolverem suas crenças a partir das mensagens recebidas.

G5.1. Quando uma chave é compartilhada entre dois (ou mais) participantes, cada um pode utilizar esse segredo para construir uma fórmula:

$$\frac{\begin{array}{l} P \lhd {}^{*}\{X\}_K,\ P \ni K,\ P \models P \overset{K}{\leftrightarrow} Q, \\ P \models \text{ø}(X),\ P \models \#(X, K) \end{array}}{P \models Q \mathrel{|\!\sim} X,\ P \models Q \mathrel{|\!\sim} \{X\}_K,\ P \models Q \ni K}$$

Se o participante P possui todas as condições a seguir,

(1) P recebe uma fórmula contendo X cifrada com a chave K e que não foi originada por ele (*) e

(2) P possui a chave K e

(3) P acredita que a chave K é um segredo satisfatório para ele e para Q e

(4) P acredita que reconhece a fórmula X e

(5) P acredita que K ou X são novos,

então P está autorizado a acreditar que: Q disse X e Q disse a fórmula X cifrada com a chave K, logo P acredita que Q possui K.

O postulado G5.2 é um exemplo de regra que permite argumentar sobre o estado do emissor.

G5.2. Se P acredita que Q disse a fórmula X e P acredita que X é novo, então P está autorizado a acreditar que Q possui X:

$$\frac{P \models Q \mid\sim X,\ P \models \#(X)}{P \models Q \ni X}$$

G6. REGRA DE JURISDIÇÃO (*Jurisdiction Rules*): este conjunto de regras mostra a autoridade que um participante possui sobre os outros participantes.

G6.1. Se P acredita que Q é uma autoridade sobre a declaração C e que Q acredita em C então P acredita em C:

$$\frac{P \models Q \Rightarrow C,\ P \models Q \models C}{P \models C}$$

G6.2. Se P acredita que Q é honesto e competente, P recebe uma mensagem contendo a extensão $(X \rightsquigarrow C)$ que ele acredita que foi dita por Q e P acredita que X é novo, então P acredita que Q realmente acredita em C.

$$\frac{P \models Q \Rightarrow Q \models *,\ P \models Q \mid\sim (X \rightsquigarrow C),\ P \models \#(X)}{P \models Q \models C}$$

Neste postulado foi incluído o termo $(X \rightsquigarrow C)$. A lógica GNY denomina C como extensão da mensagem. A extensão de uma mensagem é considerada parte da mensagem, ou seja, se um participante disse uma fórmula ele pode chegar à conclusão que ele disse a fórmula e a extensão – desde que a extensão esteja implícita na fórmula.

G7. REGRA DA RACIONALIDADE (*Rationality Rule*): declara, informalmente, que o conjunto dos postulados pode ser estendido para permitir argumentar as crenças relativas ao estado entre os participantes:

se $\frac{C1}{C2}$ é um postulado, então para qualquer participante P, $\frac{P \models C1}{P \models C2}$

3.3.2.3. ANÁLISE FORMAL

Nesta seção será apresentada a análise formal do protocolo para distribuição de chaves Needham-Schroeder. Como na análise mostrada na seção anterior, empregando a lógica BAN, a seguir será explicada de forma detalhada cada passo do protocolo utilizando a lógica GNY. E ao longo da análise será realizada a comparação entre os dois métodos.

Para dar início à análise, o protocolo será transformado numa forma idealizada. Depois serão feitas as suposições e a prova, aplicando os postulados lógicos.

- Protocolo Idealizado

1. $S \lhd {}^{*}A, {}^{*}B, {}^{*}N_a$
2. $A \lhd {}^{*}\{N_a, B, {}^{*}K_{ab}, {}^{*}\{K_{ab}, A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B\}_{Kas} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$
3. $B \lhd {}^{*}\{{}^{*}K_{ab}, {}^{*}A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$
4. $A \lhd {}^{*}\{{}^{*}N_b\}K_{ab}$
5. $B \lhd {}^{*}\{{}^{*}F(N_b)\}_{Kab} \rightsquigarrow A \models A \overset{K_{ab}}{\leftrightarrow} B$

Neste exemplo, F é uma função representando (N_b').

As suposições mostradas a seguir são ligeiramente diferentes da lógica BAN, já que os novos conceitos de posse e de reconhecimento são utilizados, porém não irão interferir no objetivo final do protocolo.

- Suposições

(1) $A \ni K_{as}$

(2) $A \ni N_a$

(3) $A \models A \overset{K_{as}}{\leftrightarrow} S$

(4) $A \models \#(N_a)$

(5) $A \models \emptyset(B)$

(6) $B \ni K_{bs}$

(7) $B \ni N_b$

(8) $B \models B \overset{K_{bs}}{\leftrightarrow} S$

(9) $B \models \#(N_b)$

(10) $B \models \emptyset(N_b)$

As suposições acima mostram que cada participante possui e compartilha uma chave secreta com a autoridade central S (suposições 1, 3, 6 e 8). Também possuem identificadores que acreditam serem novos (suposições 2, 4, 7 e 9). Além disso, A acredita que reconhece o participante B (suposição 5) e B acredita que reconhece N_b (suposição 10).

(11) $A \models S \Rightarrow (A \overset{K_{ab}}{\leftrightarrow} B)$

(12) $A \models S \Rightarrow S \models *$

(13) $A \models B \Rightarrow B \models *$

(14) $B \models S \Rightarrow (A \overset{K_{ab}}{\leftrightarrow} B)$

(15) $B \models S \Rightarrow S \models *$

(16) $B \models A \Rightarrow A \models *$

A e B acreditam que S tem jurisdição sobre as chaves de sessão que serão compartilhadas entre eles (suposições 11 e 14) e que S é honesto e competente (suposições 12 e 15). O participante A também acredita que B é honesto e competente (suposição 13) e vice-versa (suposição 16).

(17) $S \ni K_{as}$

(18) $S \ni K_{bs}$

(19) $S \ni K_{ab}$

(20) $S \models A \overset{K_{as}}{\leftrightarrow} S$

(21) $S \models B \overset{K_{bs}}{\leftrightarrow} S$

(22) $S \models A \overset{K_{ab}}{\leftrightarrow} B$

S acredita possuir chaves secretas compartilhadas entre ele e os participantes A e B (suposições 17, 18, 20 e 21). Também acredita que a chave K_{ab} é uma chave de sessão satisfatória para A e B (suposições 19 e 22).

A primeira comparação que pode ser realizada entre as duas lógicas é na quantidade de suposições utilizadas entre elas. Para a lógica BAN foram feitas doze suposições, enquanto que na lógica GNY foram vinte e duas tendo praticamente os mesmos significados. A principal diferença está na crença da lógica GNY, já que antes de acreditar numa suposição, primeiro ela deve possui-la.

- Prova

- Mensagem 1:

$S \triangleleft {}^{*}A, {}^{*}B, {}^{*}N_a$ (23)

$S \triangleleft A, B, N_a$ (24) (G1.2, 23)

Ao contrário da lógica BAN, a mensagem em texto em claro é utilizada na análise formal. S recebe a mensagem de A, aplica a regra de recebimento (G1.2) na fórmula (23) e obtém (24). Depois, aplica a regra de posse (G2.1) em (24) e obtém (25).

$S \ni (A, B, N_a)$ (25) (G2.1, 24)

Resultado: S possui A, B e N_a. Esta é a única conclusão que S poderá retirar dessa mensagem.

- Mensagem 2: pode-se notar que a extensão da mensagem $S \models A \overset{K_{ab}}{\leftrightarrow} B$ é válida, pois faz parte das suposições iniciais (suposição 22). S também tem certeza que A não pode confundir K_{ab} com uma chave secreta compartilhada entre ele e um participante que não seja B, já que o nome de B está incluído na mensagem;

$A \lhd *\{N_a, B, *K_{ab}, *\{K_{ab}, A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B\}_{Kas} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$ (26)

$A \lhd \{N_a, B, K_{ab}, \{K_{ab}, A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B\}_{Kas} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$ (27) (G1.2, 26)

$A \lhd (N_a, B, K_{ab}, \{K_{ab}, A\}_{Kbs})$ (28) (G1.3, 27 e 1)

$A \ni (N_a, B, K_{ab}, \{K_{ab}, A\}K_{bs})$ (29) (G2.1, 28)

Aplicando a regra de recebimento (G1.2) em (26), obtém-se (27). Depois, aplicando G1.3 em (27) e na suposição (1) é obtida a fórmula (28) e finalmente, utilizando a regra de posse (G2.1), obtém-se (29), ou seja, A possui todo o conteúdo da mensagem.

$A \ni K_{ab}$ (30) (G1.1, 29)

Utilizando G1.1 na fórmula (29), tem-se (30). O participante A possui a nova chave de sessão K_{ab}.

$A \models \#(N_a, B, K_{ab}, \{K_{ab}, A\}K_{bs})$ (31) (G3.1, 4)

A fórmula (31) é obtida pelo emprego da regra de recentidade (G3.1) na suposição (4). Se A acredita que o identificador (N_a) é novo e como N_a é um dos componentes da fórmula (29), então A acredita que toda a fórmula é nova (G3.1). A confia que a mensagem não é uma repetição de uma mensagem antiga (enviada numa seção anterior).

$A \models \text{ø}(N_a, B, K_{ab}, \{K_{ab}, A\}K_{bs})$ (32) (G4.1, 5)

Utilizando a regra de reconhecimento (G4.1) na suposição (5), obtém-se a fórmula (32). Como A acredita que B é reconhecível (suposição 5) , então A acredita que todo o conteúdo da mensagem é reconhecível (G4.1).

$A \models S \mid\sim (N_a, B, K_{ab}, \{K_{ab}, A\}K_{bs})$ (33) (G5.1, 26, 30, 31 e 3)

Aplicando a regra de interpretação da mensagem (G5.1) nas fórmulas (26), (30), (31), (32) e na suposição (3), obtém-se a fórmula (33). A acredita que a mensagem foi originada por S.

$A \models S \models A \overset{K_{ab}}{\leftrightarrow} B$ (34) (G6.2, 33, 12)

Empregando a regra de jurisdição (G6.2) na suposição (12) e na fórmula (33), obtém-se a fórmula (34). A acredita que S acredita que K_{ab} é uma chave de sessão satisfatória para A e B.

$A \models A \overset{K_{ab}}{\leftrightarrow} B$ (35) (G6.1, 34,11)

Aplicando a regra de jurisdição (G6.1) na suposição (11) e na fórmula (34) é obtida a fórmula (35). A acredita que K_{ab} é uma chave satisfatória para ele e B.

Resultado: A acredita que K_{ab} é uma chave satisfatória para A e B.

- Mensagem 3: Como A não possui a chave secreta K_{bs}, então ela envia a parte da mensagem cifrada com esta chave para B. A extensão da mensagem, $S \models A \overset{K_{ab}}{\leftrightarrow} B$, é válida, e por isso continua sendo mostrada.

$B \triangleleft {}_*\{{}_*K_{ab}, {}_*A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$ (36)

$B \triangleleft \{K_{ab}, A\}_{Kbs} \rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$ (37) (G1.2, 36)

$B \triangleleft K_{ab}$ (38) (G1.3, 37 e 6)

B ∋ K_{ab} (39) (G2.1)

A fórmula (37) é obtida usando a regra de recebimento (G1.2) na fórmula (36). Empregando a regra (G1.3) na fórmula (37) e na suposição (6), chega-se na fórmula (38). Finalmente, aplicando a regra de posse (G2.1), tem-se a fórmula (39), ou seja, B possui a chave K_{ab}.

Resultado: B possui a chave de sessão K_{ab}.

Comparando as duas abordagens (lógica BAN e lógica GNY), pode-se chegar à conclusão que nenhum dos postulados da lógica GNY permite derivar novas crenças ou posses da terceira mensagem, já que não pode mostrar que essa mensagem é nova. E por isso, B pode ficar preocupado com a utilização de mensagens de sessões anteriores. Ao contrário da lógica BAN, as regras da GNY não podem fornecer a conclusão que S enviou esta mensagem. Como B não está seguro que S enviou a mensagem, ou se ela é nova, então, B não pode estar convencido sobre as crenças de S e não pode fazer uso da extensão da mensagem.

- Mensagem 4: A recebe de B uma mensagem cifrada com a chave de sessão K_{ab}.

A ◁ $*\{*N_b\}_{Kab}$ (40)

A ◁ $\{N_b\}_{Kab}$ (41) (G1.2, 40)

A ◁ N_b (42) (G1.3, 41 e 30)

A ∋ N_b (43) (G2.1)

Empregando a regra de recebimento (G1.2) na fórmula (40) é obtida a fórmula (41). Aplicando (G1.3) nas fórmulas (41 e 30), obtém-se a fórmula (42) e, finalmente, utilizando a regra de posse (G2.1), tem-se a fórmula (43).
Resultado: A possui o identificador N_b.

Além de A possuir o identificador N_b, nenhuma outra conclusão pode ser encontrada. Embora a chave de sessão K_{ab} seja utilizada, A não sabe qual é a

origem da mensagem, pois não reconhece o número aleatório gerado por B e nem se B já possui a chave de sessão. A não está convencido da autenticidade do conteúdo decifrado.

- Mensagem 5: B recebe $F(N_b)$ cifrado com a chave de sessão.

$B \lhd *\{*F(N_b)\}_{Kab}$	(44)	
$B \lhd \{F(N_b)\}_{Kab}$	(45)	(G1.2, 44)
$B \lhd (F(N_b))$	(46)	(G1.3, 45 e 39)
$B \ni (F(N_b))$	(47)	(G2.1)

Aplicando a regra de recebimento (G1.2) na fórmula (44) é obtida a fórmula (45). Empregando (G1.3) nas fórmulas (45 e 39), obtém-se a fórmula (46) e, finalmente, usando a regra de posse (G2.1), chega-se na fórmula (47).

Resultado: B possui a função $F(N_b)$.

Nenhuma das regras da lógica GNY pode derivar qualquer crença ou posse da quinta mensagem. B não tem certeza se a mensagem foi enviada por A, mesmo que o conteúdo da mensagem seja acessível a B (B possui a chave de sessão K_{ab} – suposição 39) e B reconhece esse conteúdo (regra de reconhecimento G4.1 aplicada na suposição 10), B ainda não está convencido que compartilha uma chave de sessão com A, que pode ser um intruso.

- Conclusão

$A \models A \overset{K_{ab}}{\leftrightarrow} B$	(35)	
$B \ni K_{ab}$	(39)	

A conclusão indica que o participante A acredita que a chave de sessão K_{ab} é satisfatória, porém, o mesmo não ocorre com o participante B, que somente possui a chave, mas não acredita nela. Além disso, os participantes não acreditam na

crença do outro em relação a chave. Logo, o objetivo do protocolo não foi alcançado.

Diferente da lógica BAN, a lógica GNY consegue apontar o problema no protocolo Needham-Schroeder de forma mais clara, já que a única conclusão é a de que A acredita que a chave de sessão é satisfatória para ele e B.

As principais diferenças entre as abordagens, estão nos novos conceitos, nas exigências mais rígidas quando analisados os conteúdos das mensagens e, principalmente, na grande quantidade de passos que devem ser analisados em cada fase do protocolo. A TAB. 3.1 contém uma comparação das principais conclusões obtidas na análise formal realizada pelos dois métodos.

TAB. 3.1 – Comparação das Conclusões entre a Lógica BAN e GNY

Protocolo Original (Needham-Schroeder)	Protocolo Idealizado		Conclusão		Considerações
	Lógica BAN	Lógica GNY	Lógica BAN	Lógica GNY	
$A \rightarrow S: A, B, N_a$	—	$S \lhd {}^{*}A, {}^{*}B, {}^{*}N_a$	—	$S \ni (A, B, N_a)$	A primeira mensagem só foi aproveitada pela lógica GNY, já que está em texto em claro. A lógica chegou na seguinte conclusão: S possui as identidades dos participantes A e B e o identificador N_a
$S \rightarrow A:\{N_a, B, K_{ab}, \{K_{ab}, A\} K_{bs}\}K_{as} \Rightarrow \{N_a, B, K_{ab}, F\}K_{as}$	$A \lhd \{N_a, (A \overset{K_{ab}}{\leftrightarrow} B),$ $\#(A \overset{K_{ab}}{\leftrightarrow} B),$ $\{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}\}K_{as}$	$A \lhd {}^{*}\{N_a, B, {}^{*}K_{ab},$ ${}^{*}\{K_{ab}, A\}_{Kbs} \rightsquigarrow$ $S \models A \overset{K_{ab}}{\leftrightarrow} B\}_{Kas}$ $\rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$	$A \models (A \overset{K_{ab}}{\leftrightarrow} B)$ $A \models \#(A \overset{K_{ab}}{\leftrightarrow} B)$	$A \models A \overset{K_{ab}}{\leftrightarrow} B$	Na segunda mensagem os resultados foram os mesmos em ambos os métodos, mas a análise foi um pouco diferente. Como na lógica GNY existe a regra de reconhecimento, A precisava encontrar algo na mensagem que a identificasse, antes de poder analisar o seu conteúdo. Neste caso, foi declarado nas suposições que A acredita reconhecer B (suposição 5). O restante da análise foi idêntico;
$A \rightarrow B: \{K_{ab}, A\}K_{bs}$	$B \lhd \{A \overset{K_{ab}}{\leftrightarrow} B\}K_{bs}$	$B \lhd {}^{*}\{{}^{*}K_{ab}, {}^{*}A\}_{Kbs}$ $\rightsquigarrow S \models A \overset{K_{ab}}{\leftrightarrow} B$	$B \models A \overset{K_{ab}}{\leftrightarrow} B$	$B \ni K_{ab}$	Examinando a terceira mensagem, verifica-se que a lógica BAN consegue chegar na conclusão de que B acredita que a chave de sessão é satisfatória para ele e A (considerando a suposição 12 como verdadeira). Já na abordagem GNY, a única conclusão é a de que B possui a chave, não há nada novo na mensagem. B não pode ter certeza que S enviou a mensagem, porque não existe nada que B reconheça. Logo, B não está seguro de que a chave de sessão seja satisfatória;

$B \rightarrow A$: $\{N_b\}K_{ab}$	$A \lhd \{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab}$	$A \lhd *\{*N_b\}K_{ab}$	$A \models B \models A \overset{K_{ab}}{\leftrightarrow} B$	$A \ni N_b$	As duas últimas mensagens não influenciam no objetivo do protocolo. Isso pode ser observado pelos dois métodos. Na lógica BAN serviu somente para convencer ambos os participantes que eles existiam e que estavam de posse da chave de sessão. Na lógica GNY, concluiu-se que o participante A possuía o identificador, porém para ele era somente um número aleatório gerado por B e que não era reconhecido por A. Embora a chave utilizada fosse correta, A não tinha certeza da origem da mensagem;
$A \rightarrow B$: $\{N_b'\}K_{ab}$	$B \lhd \{N_b', (A \overset{K_{ab}}{\leftrightarrow} B)\}K_{ab}$	$B \lhd *\{*F(N_b)\}_{Kab} \rightsquigarrow A \models A \overset{K_{ab}}{\leftrightarrow} B$	$B \models A \models A \overset{K_{ab}}{\leftrightarrow} B$	$B \ni (F(N_b))$	A última mensagem não tem nada de útil para as duas abordagens. Na lógica GNY apesar de B reconhecer a mensagem, não pode chegar em nenhuma conclusão sobre A, já que não pode estar certo de quem enviou o identificador. Se o identificador for considerado como novo e originado por B, então o protocolo poderia ser considerado correto, ou seja, atingiu o objetivo final de distribuição da chave de sessão entre os participantes. A lógica BAN consegue atingir o objetivo considerando a suposição duvidosa 12.

De acordo com a análise realizada pelas duas lógicas, pode-se concluir que o objetivo final proposto pelo protocolo criptográfico não foi atingido. Os desenvolvedores do protocolo queriam realizar uma distribuição segura da chave de sessão entre os participantes da comunicação, o que na realidade não ocorreu. O participante A acredita que a chave é satisfatória para ele e B, porém, B não conseguiu chegar nesta conclusão. Isto foi considerado como o principal problema do protocolo e os criptoanalistas classificaram-no como falho. Em (BURROWS, ABADI e NEEDHAM, 1990) foi apresentada uma sugestão para resolver este problema.

3.4. COMPARAÇÃO E CONSIDERAÇÕES FINAIS

De acordo com o trabalho realizado foi observado que é importante a utilização de um método para a análise formal de um protocolo criptográfico. Mesmo que aparentemente o protocolo funcione, uma análise mais detalhada consegue revelar se o objetivo proposto pelo protocolo é obtido. Nesse capítulo foram vistas duas abordagens que empregam o sistema baseado em lógica modal, a lógica BAN e a lógica GNY.

A lógica BAN introduziu um método de descrição formal para idealizar e analisar protocolos criptográficos, principalmente os de autenticação e distribuição de chaves. A análise é baseada num conjunto de regras que, quando aplicadas, podem deduzir as crenças e o conhecimento dos participantes do protocolo. Existem algumas simplificações que às vezes podem ser consideradas limitações na lógica, como, por exemplo, não utilizar as mensagens em texto em claro (BOYD e MAO, 1994), e por isso, os sucessores da lógica fazem modificações buscando melhorar o método.

A lógica GNY também utiliza a definição de crença entre os participantes do protocolo. Ela é uma extensão da lógica BAN e, na tentativa de aprimorá-la, introduziu novos conceitos, como os de reconhecimento e posse e a expressão “não-originada-aqui” na qual evita o reenvio de mensagens antigas.

Além disso, a lógica GNY distingue entre posse e crença tornando-a capaz de analisar em mais níveis do que na lógica BAN. Como mostrado na TAB. 3.1, a lógica GNY através da regra de posse pode possuir uma fórmula o que não quer dizer que ela pode confiar nessa fórmula. Já a lógica BAN precisa utilizar suposições duvidosas para continuar a análise.

Apesar das vantagens, citadas acima, a lógica GNY possui desvantagens, tais como, realizar somente a autenticação, conter uma grande quantidade de postulados lógicos (são mais de cinqüenta) e ter que considerar muitas regras em cada fase do protocolo, tornando-a muito mais complexa. Alguns artigos (MATHURIA, NAINI e NICKOLAS, 1994), (MEADOWS, 1995) e (SYVERSON e CERVESATO, 2000) consideram complicada a aplicação das regras e classificam a lógica como impraticável.

O aumento da complexidade é o principal problema com os sucessores da lógica BAN na tentativa de melhorar o método. É por este motivo que a lógica BAN continua sendo a técnica mais utilizada, já que é eficiente na detecção de falhas, além de ser uma lógica simples e fácil de aplicar, como visto neste capítulo. Por causa dessas vantagens, muitos trabalhos publicados usam ou fazem referência à lógica BAN para provar a segurança dos protocolos (MYRVANG, 2000) e (AZIZ e DIFFIE, 1994).

No quarto capítulo serão mostrados três protocolos de autenticação para o ambiente de comunicação celular, onde serão descritas a troca de mensagens entre os participantes, o funcionamento destes protocolos e os objetivos de segurança propostos. Com a finalidade de observar se as metas dos protocolos são alcançadas, será feita a análise formal empregando a lógica BAN.

4. ANÁLISE DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDE CELULAR

4.1. INTRODUÇÃO

O objetivo principal dos sistemas de comunicação móvel pessoal é fornecer acesso aos serviços de telecomunicações em qualquer parte. Para isso, os projetistas precisam superar os desafios encontrados como, por exemplo, o acesso de assinantes não autorizados aos recursos da rede. Essa proteção só é conseguida através do uso de técnicas criptográficas e controle de acesso (MOLVA, SAMFAT e TSUDIK, 1994).

A preocupação com a segurança é maior nos sistemas de comunicação sem fio, pois o meio é mais suscetível a ataques do que nos sistemas cabeados. No meio sem fio, qualquer um, com um equipamento apropriado, pode escutar tudo que está sendo enviado na rede, podendo obter informações importantes e sigilosas, tais como as chaves secretas, e dessa forma, ter acesso aos recursos dos assinantes legítimos da rede. Além disso, é praticamente impossível perceber a presença de um intruso no canal de comunicação. Por estes motivos, a segurança realiza uma função vital para o êxito das operações num sistema de comunicação móvel.

Nos sistemas de primeira geração (1G) AMPS, um intruso conseguia invadi-lo usando equipamentos simples que podiam ser construídos sem muito esforço (RAMASAMI, 2000). Por isso, os sistemas de segunda geração (2G) começaram a se preocupar com os aspectos de segurança. O GSM foi o pioneiro na criação de um protocolo de autenticação que tem como objetivo fornecer autenticação do usuário e a distribuição de uma chave de sessão para ser utilizada durante a comunicação.

O problema é que os protocolos estão sujeitos a erros no desenvolvimento e por isso é importante que seja empregado algum método formal (seção 2.5 do segundo capítulo) para avaliar se os objetivos propostos pelos desenvolvedores foram alcançados.

Neste capítulo será realizada a análise de alguns dos principais protocolos de autenticação do sistema de comunicação móvel celular: GSM, CDPD e UMTS. Como técnica será empregada a lógica BAN (ver terceiro capítulo) a fim de proporcionar uma base formal e determinar a utilidade do protocolo. Baseada nesta análise, podem ser tiradas conclusões sobre a segurança fornecida pelo protocolo.

O uso da lógica BAN permite uma identificação mais precisa dos problemas de segurança e mostra se os objetivos foram atingidos. Embora a segurança oferecida por dois dos protocolos mencionados já tenham sido examinadas em (GODFREY, 1995) uma análise do UMTS e dos três protocolos como um grupo não foi realizada.

Este trabalho, ao contrário de (GODFREY, 1995), apresenta uma notação diferente e mais simples, faz uma análise detalhada e explica de forma clara cada passo do protocolo. Além disso, a comparação entre as lógicas BAN e GNY realizada no terceiro capítulo ajuda a esclarecer as falhas encontradas e serve como base para as conclusões.

O quarto capítulo está organizado da seguinte forma: a seção 4.1.1 contém os propósitos de segurança que os protocolos de autenticação devem fornecer; a seção 4.1.2 relaciona a notação básica e a seção 4.1.3 os postulados lógicos usando uma representação mais intuitiva do que mostrado no terceiro capítulo; a seção 4.2 descreve o sistema celular móvel GSM; a seção 4.3 mostra o sistema CDPD e a seção 4.4 descreve o sistema de terceira geração UMTS, nestas seções são mostrados os protocolos de autenticação utilizados pelos sistemas, os fluxos de mensagens, os serviços de segurança e é feita a análise formal, empregando a lógica BAN. Finalmente, na seção 4.5 são feitas as considerações finais do capítulo.

4.1.1. PROPÓSITOS DE SEGURANÇA

Antes de ser iniciada a descrição dos protocolos criptográficos, serão relacionados os principais objetivos de segurança a serem alcançados por eles (LIN, HARN, 1995) e (LIN e HARN, 1999). Estes objetivos podem apresentar variações específicas de acordo com as descrições apresentadas no decorrer da seção:

- fazer o meio rádio tão seguro quanto a rede fixa a fim de protegê-la contra invasões, o que implica no anonimato da identidade e no sigilo das informações dos participantes;
- ter uma autenticação satisfatória, prevenindo a ocorrência de fraudes contra os participantes;
- ter certeza que as faturas foram enviadas aos assinantes corretos e que os serviços não estão comprometidos;
- impedir que as redes operadoras comprometam a segurança entre si (inadvertidamente ou por competitividade);
- a implementação da segurança:
    - não deve exigir um aumento da largura de banda do canal;
    - não deve acrescentar um atraso significativo na inicialização de chamada e nem nas comunicações subseqüentes;
    - deve ter custo efetivo;
    - não deve permitir um aumento na taxa de erro;
    - não deve acrescentar uma complexidade excessiva ao resto do sistema.

4.1.2. NOTAÇÃO BÁSICA

Nesta seção será descrita a notação empregada na descrição dos protocolos de autenticação, padronizando e facilitando o entendimento e a análise formal.

Os componentes da notação podem ser divididos em três categorias: os participantes, os algoritmos criptográficos e as informações do protocolo.

Cada protocolo possui ao menos duas entidades que são os participantes envolvidos na comunicação atual. Para simplificar, serão denominadas: A como os terminais móveis e B como o outro ponto final da conexão (por exemplo, as estações base). Em alguns protocolos são encontradas uma terceira parte confiável, que embora tenha funcionalidades similares, recebem nomes diferentes, tais como autoridade certificadora, autoridade de autenticação, autoridade central etc. Neste trabalho será designada de Autoridade Central (AC) a entidade que fornece segurança e/ou as informações de identificação.

K_X = chave pública de X (sistema criptográfico de chave assimétrica); usada na operação de ciframento;

K_X^{-1} = chave privada de X (sistema criptográfico de chave assimétrica; usada na operação de deciframento e para assinatura digital;

K_{XY} = chave secreta conhecida somente por X e Y do sistema criptográfico de chave simétrica; usada tanto para o ciframento quanto para o deciframento. Essa notação pode ser empregada também para a chave de sessão negociada durante a comunicação entre os participantes X e Y;

N_X = (identificadores) número aleatório gerado por X;

Para a representação e análise dos protocolos será adotada a notação mostrada em dois (2), por ser mais intuitiva do que a apresentada no terceiro capítulo. Por exemplo, compare as seguintes expressões (a primeira é a notação da lógica BAN original):

1. $P \models Q \sim \#(X)$
2. P **acredita** Q **disse novo**(X)

(lê-se: P acredita que Q, há algum tempo, disse que X é nova)

A lógica BAN consiste nas seguintes expressões:

1. P **acredita** X: o participante P acredita na fórmula X ou está autorizado a acreditar em X, isso significa que P pode agir como se X fosse verdadeira;
2. P **recebeu** X: P recebeu uma mensagem contendo X e P pode obter X da mensagem (normalmente depois de algum deciframento);
3. P **disse** X: P uma vez disse X. O participante P, há algum tempo, enviou uma mensagem contendo a fórmula X;
4. P **controla** X: P tem jurisdição sobre X. O participante P é uma autoridade sobre X e deve ser confiado deste modo;
5. **novo**(X): (lê-se “X é nova”) a fórmula X é nova, ou seja, a fórmula X não foi usada numa mensagem anterior à execução atual do protocolo. Os identificadores são gerados com a finalidade de serem novos;
6. $P \overset{k}{\leftrightarrow} Q$: (lê-se “k é uma chave satisfatória para P e Q”). A chave k nunca será descoberta por qualquer participante, exceto por P, Q ou por alguém em quem eles confiam;

7. $\mapsto^{k}$ P: P possui como chave pública k. A correspondente chave privada k^{-1} é conhecida somente por P ou pelo participante em quem ele confia;
8. P $\rightleftharpoons^{X}$ Q: A fórmula X é um segredo conhecido somente por P e Q e, possivelmente, pelo participante em quem eles confiam. X pode ser utilizada somente por P ou Q para provar suas identidades. A fórmula X é tão nova quanto secreta;
9. $\{X\}_K$: fórmula X cifrada com a chave K. As mensagens cifradas somente são legíveis e verificáveis pelo possuidor da chave.
10. <X>Y: representa a combinação da fórmula X com a fórmula Y. Esta representação só é utilizada quando o segredo é solicitado como uma prova de identidade.

A notação abaixo é usada numa troca de mensagem:

$$\text{Mi} \quad A \rightarrow B: \{X\}_k$$

onde i é a iésima mensagem do protocolo: A envia X cifrada com a chave k para B.

Em todas estas expressões, X é uma mensagem ou uma fórmula. Como será visto, toda fórmula pode ser uma mensagem, mas nem toda mensagem é uma fórmula.

4.1.3. POSTULADOS LÓGICOS

Da mesma forma que na notação básica, será utilizada uma representação mais intuitiva dos postulados. Existem quatro postulados (ou regras) principais na lógica BAN utilizados para verificar se o protocolo está correto:

B1. Regra de significado da mensagem:

$$\frac{P \textbf{ acredita } P \leftrightarrow^{k} Q,\ P \textbf{ recebeu } \{X\}_k}{P \textbf{ acredita } Q \textbf{ disse } X}$$

Se P recebeu X cifrada com a chave k e se P acredita que k é uma chave satisfatória para se comunicar com Q, então P acredita que Q uma vez disse X.

B1.1. Para chave pública:

$$\frac{P \textbf{ acredita } \mapsto^{k} Q,\ P \textbf{ recebeu } \{X\}_{k}^{-1}}{P \textbf{ acredita } Q \textbf{ disse } X}$$

Se P recebeu X cifrada com a chave privada de Q e P acredita que K é a chave pública de Q, então P acredita que Q uma vez disse X.

Uma notação semelhante pode ser utilizada para segredos compartilhados (terceiro capítulo, seção 3.3.1.2)

B2. Regra de verificação do identificador:

$$\frac{P \textbf{ acredita novo}(X),\ P \textbf{ acredita } Q \textbf{ disse } X}{P \textbf{ acredita } Q \textbf{ acredita } X}$$

Se P acredita que a fórmula X é nova e que Q uma vez disse X, então P também acredita que Q acredita em X. Como P **acredita novo**(X) e **novo**(X) isso significa que a fórmula X nunca foi utilizada anteriormente. P também acredita que Q nunca disse a fórmula X antes (durante a execução da sessão atual do protocolo).

B3. Regra de Jurisdição:

$$\frac{P \textbf{ acredita } Q \textbf{ controla } X,\ P \textbf{ acredita } Q \textbf{ acredita } X}{P \textbf{ acredita } X}$$

Nem sempre é suficiente para P acreditar que Q acredita numa fórmula. A regra de jurisdição indica que P acredita na fórmula X, se P acredita que Q tem jurisdição sobre X.

Com essas regras e com a notação mostrada anteriormente, as crenças de todos os participantes do protocolo podem ser declaradas. Para maiores detalhes ver terceiro capítulo.

4.2. GSM

O GSM é um sistema celular móvel digital de padrão europeu e foi o pioneiro a fornecer serviços de segurança como a autenticação do usuário, sigilo e distribuição da chave de sessão (LIN, HARN e KUMAR, 1995). É um dos sistemas celulares de segunda geração mais utilizados no mundo, baseado numa combinação dos protocolos de acesso TDMA[13] (*Time Division Multiple Access*) e FDMA[14] (*Frequency Division Multiple Access*) (RAMASAMI, 2000).

Os dados referentes à assinatura e identificação do assinante não estão incorporados ao aparelho celular, mas a um cartão (*chip*) destacável denominado SIM (*Subscriber Identity Module*). Este SIM contém a chave secreta (K_{ac}) conhecida somente por ele e pelo HLR (*Home Location Register*), a identidade internacional do assinante móvel IMSI – (*International Mobile Station Identity*), pode incluir o número de identidade pessoal – PIN (*Personal Identification Number*) e outros dados relevantes ao assinante (MOULY e PAUTET, 1992).

O GSM é baseado no sistema criptográfico de chave simétrica e utiliza como processo de autenticação um mecanismo de desafio-resposta. Para realizar os requerimentos de segurança, mencionados na seção 4.2.1 a seguir, são utilizados três algoritmos: A8, A5 e A3. O A8 é o algoritmo empregado para gerar a chave de sessão usada entre as partes para cifrar o conteúdo das mensagens trocadas após a autenticação. O A3 é o algoritmo usado para gerar o desafio-resposta, tendo como entrada o número aleatório gerado pela rede e a chave secreta. O A5 é o algoritmo

---

[13] TDMA – Método de compartilhamento de uma freqüência entre vários usuários pela divisão da freqüência em intervalos de tempo discretos (DORNAN, 2001).

[14] FDMA – Método de espectro de compartilhamento entre usuários dividindo-o em canais distintos (DORNAN, 2001).

utilizado para o ciframento/deciframento do fluxo de dados usando a chave de sessão (MEHROTRA e GOLDING, 1998).

Os principais elementos da arquitetura da rede GSM compreendem (FIG. 4.1):

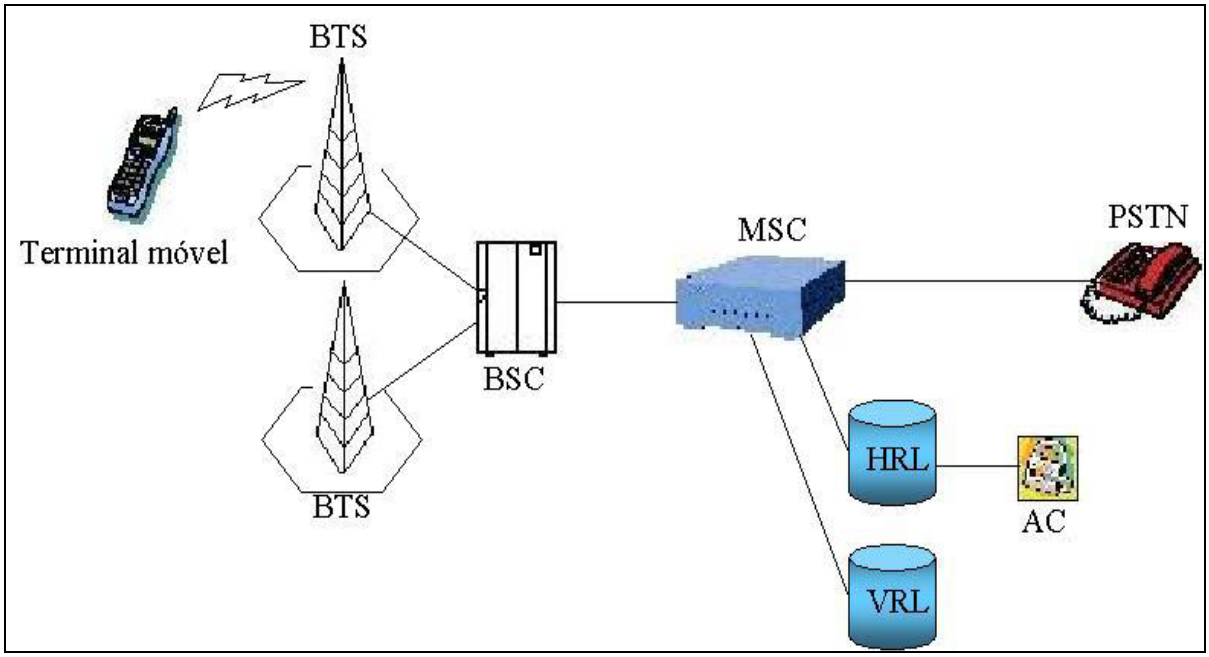

FIG. 4.1 – Arquitetura da Rede GSM

- terminal móvel: é o equipamento referente aos dispositivos portáteis suportados pelo sistema GSM;
- MSC (*Mobile Services Switching Center*): é onde se executam as funções de comutação, interface com a rede, sinalização, cobrança dos serviços e unidade para interoperabilidade com a rede fixa PSTN. O MSC coordena também o tráfego com outras redes celulares;
- HLR (*Home Location Register*): é um banco de dados que armazena e gerencia as informações referentes aos assinantes e às assinaturas (dados permanentes tais como: tipos de assinatura e acesso a serviços suplementares). Pode estar separado ou integrado ao MSC. Os assinantes "visitantes" não são tratados pelo HLR e sim pelo banco de dados anexo à própria MSC, denominado VLR (*Visitor Location Register*);
- VLR: é um banco de dados com as informações de celulares de outras áreas de serviço que, no momento, estão transitando na área desse MSC;

- autoridade central - AC: é responsável pelos parâmetros de autenticação e ciframento das mensagens, a fim de proteger a identidade do assinante transmitida na interface aérea e assegurar o sigilo das ligações;
- estação base: tem como função interconectar os terminais móveis entre si. Está conectada ao MSC através do enlace cabeado e com os terminais móveis através de rádio. Na arquitetura é representada pela BTS (*Base Transceiver Station*) e BSC (*Base Station Controller*).

4.2.1. OBJETIVOS DO PROTOCOLO

De acordo com os propósitos de segurança foram definidos os seguintes serviços no GSM a fim de evitar o abuso da rede e fornecer sigilo aos assinantes (RAMASAMI, 2000):

- autenticação da identidade do assinante: o assinante tem que provar sua identidade ao sistema antes de qualquer transação ser feita. Se suspeitar da identidade temporária (TMSI – *Temporary Mobile Subscriber Identity*) do assinante, o HLR requisita a identidade legítima do móvel. Se a autenticação falhar repetidamente, o VLR também solicita ao móvel a sua identidade legítima. A autenticação da identidade tem a finalidade de evitar o abuso dos serviços pelos assinantes autorizados. Este serviço pode ser iniciado toda vez que um assinante acessar o sistema;
- sigilo da identidade do assinante: toda vez que o assinante muda de área de localização, uma nova identidade temporária é calculada pelo HLR/VLR, cifrada e enviada para o terminal móvel. Essa identidade só é válida numa determinada área de localização. Uma identidade temporária é dada ao móvel para evitar a possibilidade de invasões utilizando uma identidade legítima ou identidades temporárias antigas;
- sigilo dos dados de sinalização: o fluxo de dados de sinalização é cifrado e decifrado usando o algoritmo de ciframento A5 e a chave de sessão compartilhada;

- sigilo dos dados do usuário: da mesma forma que no fluxo de dados de sinalização, é realizado o ciframento e o deciframento utilizando o algoritmo *A5* e a chave de sessão compartilhada;
- distribuição da chave de sessão: a chave de sessão é calculada pelo terminal móvel e pelo HLR/VLR através do desafio-resposta, utilizando o algoritmo A8. Essa chave é trocada a cada sessão. Dessa forma, evita-se que um intruso consiga obter uma chave durante a execução atual do protocolo e tente utilizá-la em comunicações posteriores.

4.2.2. FLUXO DE MENSAGENS

Quando o móvel (A) está em sua área de registro e quer se comunicar, precisa ser autenticado pelo HLR (B) enviando sua identidade temporária (A'). B responde com um desafio. Se o móvel responder com o valor correto ($\{N_b\}K_{ab}$) então é autenticado e a operação é executada com êxito. O protocolo de autenticação é mostrado na FIG. 4.2.

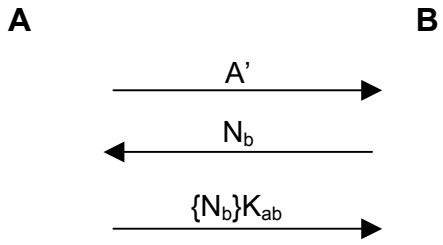

FIG. 4.2 – Protocolo de Autenticação do GSM

Devido a mobilidade, existe uma grande possibilidade do terminal móvel requerer serviço num outro domínio que não seja a da sua rede. Neste caso, a rede servidora terá que negociar com o terminal móvel visitante. Para B poder autenticar A, precisa contatar C, através do *backbone* cabeado, obter o desafio-resposta e a chave de sessão (FIG. 4.3).

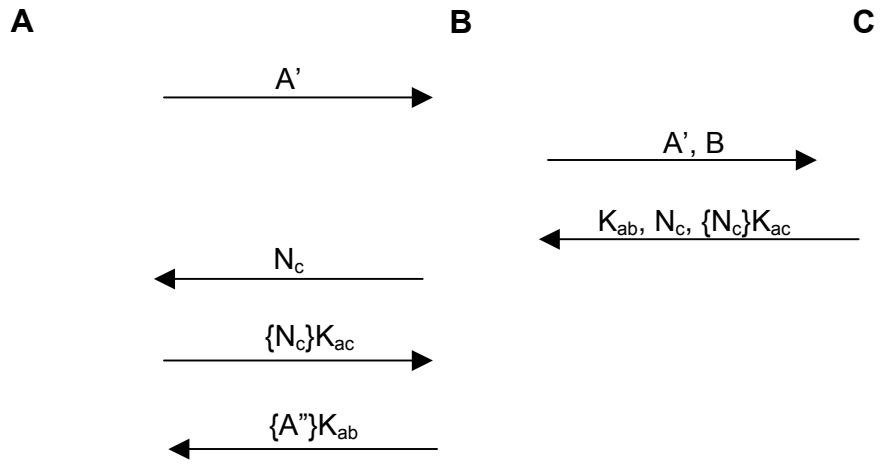

FIG. 4.3 – Protocolo de Autenticação do GSM
(móvel fora da área de registro)

1º Passo: A envia sua identidade temporária (A') para B;

2º Passo: B repassa para C a própria identidade e a identidade temporária recebida;

3º Passo: C recebe da autoridade central uma tripla contendo os componentes (N_C, $\{N_c\}K_{ac}$, K_{ab}) e envia-os a B.

A chave de sessão é calculada da seguinte forma: $K_{ab} = A8(\{N_c\}K_{ac})$.

4º Passo: para verificar a identidade de A, B envia o N_c como desafio a ele;

5º Passo: A responde com o $\{N_c\}K_{ac}$. B verifica se a resposta ao desafio está correta, comparando com o recebido de C na terceira mensagem. Se for o valor esperado, então ele acredita que está se comunicando com um assinante legítimo e que a autenticação foi feita com sucesso. Desse modo, o móvel pode continuar a comunicação. Caso contrário, a conexão é liberada e uma indicação é enviada ao móvel, avisando-o que a autenticação não foi realizada com sucesso;

6º Passo: B envia a A uma nova identidade temporária (A") cifrada com a chave de sessão K_{ab} usando o algoritmo A5. Essa identidade será utilizada na próxima sessão;

Observe que neste ponto, A ainda não tem certeza que B tem a mesma chave de sessão, pois o N_c recebido pode não ter vindo de um VLR legítimo. O protocolo GSM realiza outra rodada de troca de mensagens para assegurar que ambas as partes têm a mesma chave de sessão secreta compartilhada. Isto demonstra uma fraqueza com o protocolo, pois apesar de garantir aos dois participantes a posse da

chave de sessão (K_{ab}), a outra rodada não impede que outros também tenham a chave, já que esta é transmitida em claro no enlace cabeado.

Só depois que estes passos são completados, é que A e B se comunicam cifrando a mensagem com o algoritmo A5 e utilizando a chave de sessão K_{ab}.

Para cada chamada subseqüente, A usa uma identidade temporária, escondendo assim, a sua identidade legítima e dentro de cada rodada de autenticação, uma nova identidade temporária é selecionada e transmitida a ele. Já que cada identidade temporária é transmitida ao assinante em texto cifrado e somente ele pode decifrá-lo, então, ele pode utilizá-la como prova de identidade para a rede.

4.2.3. ANÁLISE FORMAL

Além da notação utilizada, do detalhamento e das explicações realizadas, este trabalho apresentou uma análise distinta da encontrada em (GODFREY,1995). Foram aplicados outros postulados nas análises realizadas nos protocolos de autenticação do GSM e CDPD, e conseqüentemente, feitas novas suposições. As conclusões obtidas foram as mesmas; a principal diferença é que Godfrey empregou o postulado (B1.3) e essa análise utiliza o postulado (B1.1) nas provas. Isto mostra uma validação do trabalho de Godfrey e a certeza das fraquezas encontradas no GSM e no CDPD. Outra diferença é que este trabalho considera a sexta mensagem do protocolo de autenticação do GSM na análise já que faz parte dos serviços de segurança (sigilo da identidade do usuário).

- Protocolo

M1: $A \rightarrow B$ A'

M2: $B \rightarrow C$ A', B

M3: $C \rightarrow B$ $K_{ab}, N_c, \{N_c\}K_{ac}$

M4: $B \rightarrow A$ N_c

M5: $A \rightarrow B$ $\{N_c\}K_{ac}$

M6: B $\rightarrow$ A $\{A''\}K_{ab}$

- Protocolo Idealizado

M3 C $\rightarrow$ B $(A \overset{K_{ab}}{\leftrightarrow} B, N_c, \{N_c\}K_{ac}, \textbf{novo}\{N_c\}_{K_{ac}})$

M4 B $\rightarrow$ A N_c

M5 A $\rightarrow$ B $\{N_c\}K_{ac}$

M6 B $\rightarrow$ A $\{$ **novo** A$\}K_{ab}$

- Suposições

1) A **acredita** $A \overset{K_{ac}}{\leftrightarrow} C$

2) C **acredita** $A \overset{K_{ac}}{\leftrightarrow} C$

3) A **acredita** C **controla** $A \overset{K_{ab}}{\leftrightarrow} B$

4) B **acredita** C **controla** $A \overset{K_{ab}}{\leftrightarrow} B$

5) A **acredita** C **disse** N_c

6) B **acredita** A **disse** $\{N_c\}K_{ac}$

7) B **acredita** C **controla** $(A \overset{K_{ab}}{\leftrightarrow} B, N_c, \{N_c\}K_{ac}, \textbf{novo}\ \{N_c\}K_{ac})$

8) B **acredita** C **acredita** $(A \overset{K_{ab}}{\leftrightarrow} B, N_c, \{N_c\}K_{ac}, \textbf{novo}\ \{N_c\}K_{ac})$

As suposições 7 e 8 são baseadas na confiança que o enlace cabeado é seguro.

- Prova

Mensagem 3:

B **recebeu** $(A \overset{K_{ab}}{\leftrightarrow} B, N_c, \{N_c\}K_{ac}, \textbf{novo}\{N_c\}_{K_{ac}})$ (9)

B **acredita** $(A \overset{K_{ab}}{\leftrightarrow} B, N_c, \{N_c\}K_{ac}, \textbf{novo}\{N_c\}_{K_{ac}})$ (10) (B3, 7,8)

B **acredita** N_c (11) (B4, 10)

B **acredita** $\{N_c\}K_{ac}$ (12) (B4, 10)

B **acredita novo**$\{N_c\}_{K_{ac}}$ (13) (B4, 10)

B **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$ (14) (B4, 10)

B recebe toda a fórmula (9). Aplicando a regra de jurisdição (B3) nas suposições (7) e (8) (confiança no enlace cabeado) ele obtém a fórmula (10). Depois, empregando a regra (B4) em (10), obtém as fórmulas (11), (12), (13) e (14). As fórmulas (12) e (13) serão úteis na análise da quinta mensagem. Essas fórmulas indicam que B acredita que A e C possuem um segredo e que este segredo é novo. Além disso, este segredo é usado para autenticar A. A fórmula (14) indica a distribuição da chave de sessão K_{ab}.

Resultado: B obtém a chave de sessão K_{ab} de C.

Mensagem 4:

A **recebeu** (N_c) (15)

A **acredita** C **disse** N_c (5)

A **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$ (16) $K_{ab} = A8(\{N_c\}K_{ac})$

A recebe N_c e pode calcular a chave de sessão K_{ab}.

Resultado: A acredita que C há algum tempo disse N_c.

O número aleatório N_c será utilizado pelo participante A para gerar a chave de sessão e a resposta ao desafio recebido. A chave de sessão é produzida através do ciframento de N_c com o algoritmo A8 usando a chave K_{ac} (16). A resposta ao desafio é gerada através do ciframento de N_c com o algoritmo A5 utilizando a chave K_{ac}.

Como a lógica BAN não contém o conceito de posse (como a da lógica GNY) definido por A **possui** N_c, a análise recorre a suposição duvidosa (5) A **acredita** C **disse**

N_c. Porém, A não pode ter certeza que esse N_c veio de C já que foi recebido de outro participante, neste caso, B. Se B for um intruso e estiver de posse da chave secreta que A compartilha com C, então, poderá obter todas as informações de A.

O GSM, na realidade, transmite o N_c para que o participante A, através dos algoritmos A5 e A8, possa gerar internamente a chave de sessão (K_{ab} = A8($\{N_c\}k_{ac}$ e a resposta ao desafio = A5($\{N_c\}k_{ac}$). Evitando transmitir estas informações (por exemplo, a chave de sessão) na rede.

Mensagem 5:

B **recebeu** $\{N_c\}K_{ac}$	(17)
B **acredita novo** $\{N_c\}K_{ac}$	(13)
B **acredita** A **acredita** $\{N_c\}K_{ac}$	(18) (B2, 13, 6)

B recebe a fórmula (17) e como possui a fórmula (13) pode realizar a autenticação de A da seguinte forma: aplicando a regra de verificação do identificador (B2) usando (13) e (6) obtendo (18).

Resultado: B autentica A.

A quinta mensagem é utilizada por B para autenticar o terminal móvel A. Se a resposta ao desafio for igual ao valor recebido na terceira mensagem, então o móvel A é um usuário legítimo e a autenticação foi realizada com êxito. Além disso, B também acredita que A pode gerar a chave de sessão.

B agora envia uma identidade temporária que será usada por A para esconder sua identidade legítima. Isso atende a um dos requisitos de segurança, o sigilo da identidade do participante.

Mensagem 6:

A **recebeu** { **novo** A}K_{ab}	(19)
A **acredita** B **disse novo** A	(20) (B1, 19, 16)

B recebe a fórmula (19) e aplicando a regra de significado da mensagem (B1) nas fórmulas (19) e (16) obtém (20).

Resultado: A obtém sua nova identidade temporária.

Para as comunicações posteriores, A irá utilizar a identidade temporária e a chave de sessão compartilhada entre ele e B para cifrar/decifrar as mensagens, usando o algoritmo A3.

- Conclusão

B **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$	B obtém a chave de sessão
A **acredita** C **disse** N_c	A não está convencido que N_c é novo
B **acredita** A **acredita** $\{N_c\}K_{ac}$	B autentica A
A **acredita** B **disse novo** A	A obtém a nova identidade temporária

A análise pela lógica BAN mostra que B crê que a chave de sessão compartilhada com A é satisfatória, porém o participante A não está convencido que essa chave é nova (já que o N_c é utilizado como semente para a geração dela). B também acredita que A respondeu com o valor correto ao desafio gerado por C, logo A é um usuário legítimo.

De acordo com a análise realizada neste trabalho, os objetivos definidos pelos desenvolvedores do protocolo em autenticar o terminal móvel e fornecer a distribuição segura de uma chave de sessão, não são completamente satisfeitos. O móvel é autenticado pela estação base usando um desafio recebido do HLR, porém, apesar da chave de sessão ser distribuída, existe uma fraqueza no desafio apresentado ao móvel: o terminal móvel não é capaz de determinar quem enviou o desafio e se ele é novo. Conseqüentemente não pode estar certo se a chave gerada é atualmente válida. Apesar de não ser evidente, esta fraqueza pode ser aproveitada por um intruso.

Outro problema com os serviços de segurança no GSM é que ele depende da suposição que o *backbone* cabeado é seguro. Numa grande rede global, esta

suposição é muito difícil de ser atingida. Um intruso pode obter uma cópia da tripla (desafio, número aleatório e chave de sessão) enviada e, dessa forma, poderá se passar pela base indefinidamente. Por este motivo, é importante que seja implementado algum protocolo de segurança entre as estações base e o HLR.

4.3. CDPD

O sistema CDPD foi desenvolvido por um consórcio de várias companhias norte-americanas, inicialmente projetado para o transporte de pacotes de dados sobre a rede celular analógica existente (AMPS) utilizando os canais livres de comunicação de voz (ASOKAN, 1995).

Da mesma forma que no GSM, o meio de transmissão é suscetível a ataques e por isso, o CDPD fornece serviços de segurança incluindo o sigilo dos dados, a distribuição de uma chave de sessão e a autenticação da unidade móvel (JOSEPH, 2000).

A rede CDPD é composta pelas seguintes entidades (FIG. 4.4).

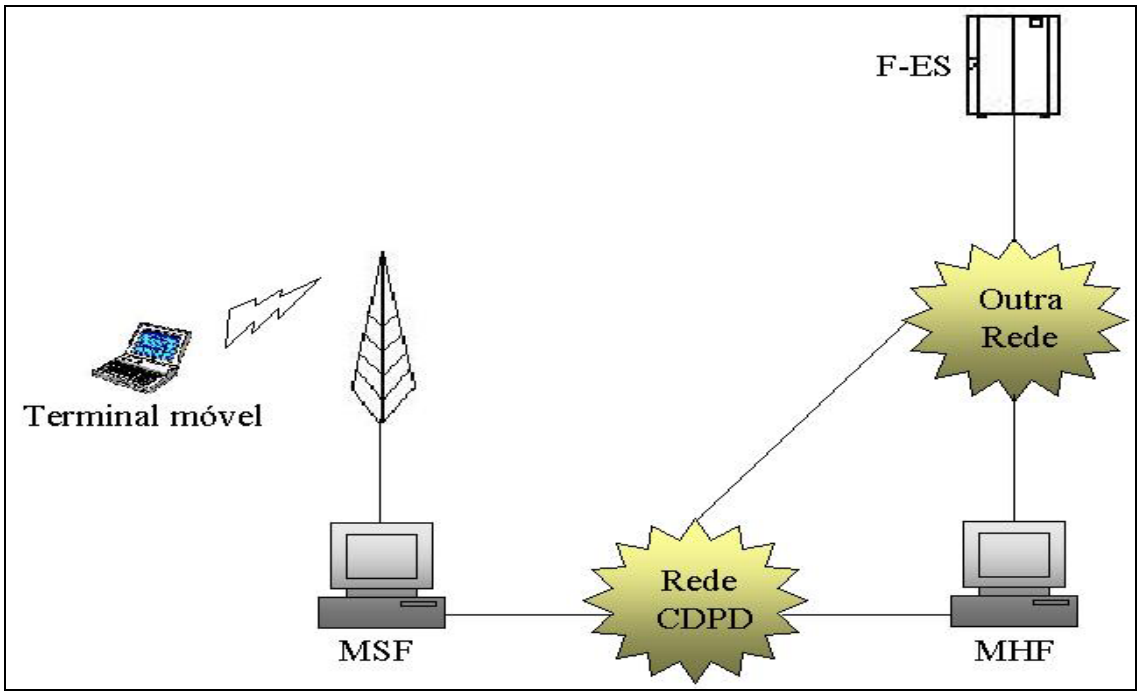

FIG. 4.4 – Arquitetura da Rede CDPD

- terminal móvel (M-ES – *Mobile End System*): é um computador móvel que acessa a rede CDPD através do enlace de rádio. Para cada móvel é nomeado um NEI (*Network Entity Identifiers*);
- estação base (MDBS – *Mobile Data Base Station*): faz a interface entre os terminais móveis e a rede servidora. Está conectada aos móveis pelo enlace rádio e pela rede cabeada ao MSF.
- MHF (*Mobile Home Function*) e MSF (*Mobile Serving Function*): são entidades que executam as funções de roteamento;
- F-ES (*Fixed End System*): rede fixa conectada ao MHF através do *backbone* cabeado.

Cada móvel possui um nome único (NEI) e pertence a um domínio (MHF) onde foi registrado. Para se autenticar frente ao MHF, o móvel (A) precisa apresentar uma tripla <A, ARN, ASN> recebida durante o processo de registro.

ARN = *Authentication Record Number*

ASN = *Authentication Sequence Number*.

Se a autenticação for executada com sucesso, então o MHF gera novos valores para ARN e ASN e os envia a A. Na próxima comunicação, o móvel deverá utilizar esses novos valores.

4.3.1. OBJETIVOS DO PROTOCOLO

O protocolo de autenticação é executado durante a inicialização da chamada e durante os *handoffs*. Possui um mecanismo simples para manter o sigilo da identidade, enquanto fornece o controle de acesso (PARK, 1996) e (FRANKEL, 1995):

- autenticação da identidade do assinante: antes de qualquer transação ser feita, o assinante tem que provar sua identidade para sua rede de registro (MHF). De acordo com os parâmetros enviados, o sistema aceita ou rejeita a solicitação da comunicação;

- sigilo dos dados do usuário: é realizado o ciframento e o deciframento utilizando o algoritmo RC-4 (SCHNEIER, 1996) e a chave de sessão compartilhada K_{ab}.

4.3.2. FLUXO DE MENSAGENS

Para o fluxo de mensagens mostrado na FIG. 4.5, supõe-se que o terminal móvel está fora da sua área de registro.

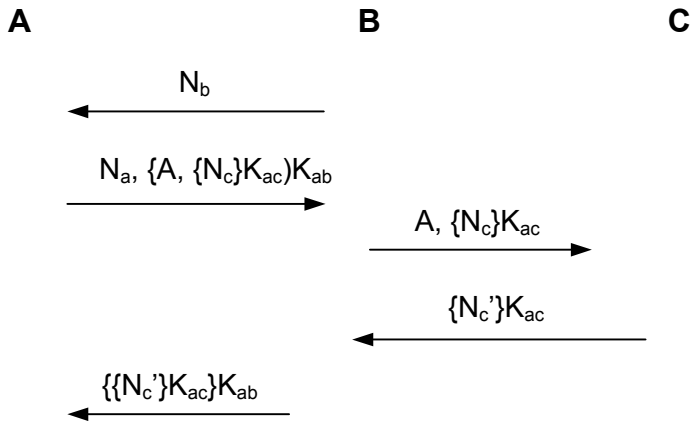

FIG. 4.5 – Protocolo de Autenticação do CDPD

O processo inicia com a troca de chaves Diffie-Hellman (ver segundo capítulo) entre o móvel A e a rede servidora B, gerando a chave de sessão K_{ab} que será compartilhada entre eles. O protocolo Diffie-Hellman permite que os participantes de uma conexão, sobre um canal inseguro, negociem uma chave compartilhada de forma que um intruso não possa determiná-la.

1º passo: B envia um número aleatório N_b que servirá como parte da chave de sessão;
2º passo: A recebe N_b, gera N_a e calcula a chave de sessão $K_{ab} = N_a \bullet N_b$. O N_a será enviado para B para calcular também a chave de sessão. Estabelecida a chave de sessão, A apresenta suas credenciais para B, ou seja, submete o NEI (*Network Equipment Identifier*), representado no fluxo de mensagens por A, e o SHR (*Shared*

Historical Record) composto dos valores ARN e ASN, representado no fluxo de mensagens por N_c, tudo cifrado pelo algoritmo RC4 (SCHNEIER, 1996) usando a chave de sessão, K_{ab}. Esta tripla servirá para C autenticar A;

3º passo: se A estiver fora de seu domínio de registro, então as credenciais são repassadas para C em texto em claro (confiança na rede cabeada);

4º passo: C valida as credenciais e envia uma mensagem de confirmação para B junto com o novo SHR, representado no fluxo de mensagens por N_c';

5º passo: B cifra N_c' com a chave de sessão K_{ab} e envia para A.

4.3.3. ANÁLISE FORMAL

- Protocolo

M1: $B \rightarrow A$ N_b

M2: $A \rightarrow B$ N_a, $\{A, \{N_c\}K_{ac}\}K_{ab}$

M3: $B \rightarrow C$ A, $\{N_c\}K_{ac}$

M4: $C \rightarrow B$ $\{N_c'\}K_{ac}$

M5: $A \rightarrow B$ $\{\{N_c'\}K_{ac}\}K_{ab}$

- Protocolo Idealizado

M1 $B \rightarrow A$ $A \overset{N_b}{\leftrightarrow} B$

M2 $A \rightarrow B$ $A \overset{N_a}{\leftrightarrow} B$, $\{\{N_c\}K_{ac}\}K_{ab}$

M3 $B \rightarrow C$ $\{N_c\}K_{ac}$

M4 $C \rightarrow B$ **novo**$\{N_c\}K_{ac}$

M5 $B \rightarrow A$ { **novo**$\{N_c\}K_{ac}\}K_{ab}$

- Suposições

1. A **acredita** B **controla** $A \overset{N_b}{\leftrightarrow} B$
2. B **acredita** A **controla** $A \overset{N_a}{\leftrightarrow} B$
3. B **acredita** A **acredita** $A \overset{N_a}{\leftrightarrow} B$
4. A **acredita** B **acredita** $A \overset{N_b}{\leftrightarrow} B$
5. A **acredita** B **disse** N_b
6. B **acredita** A **disse** N_a
7. C **acredita** $A \overset{K_{ac}}{\leftrightarrow} C$
8. A **acredita** $A \overset{K_{ac}}{\leftrightarrow} C$
9. C **acredita novo**N_c
10. B **acredita** C **acredita** (**novo**$\{N_c\}K_{ac}$)
11. B **acredita** C **controla** (**novo**$\{N_c\}K_{ac}$)

As suposições 10 e 11 são baseadas na confiança que o enlace cabeado é seguro.

- Prova

Mensagem 1:

A **recebeu** $A \overset{N_b}{\leftrightarrow} B$	(12)
A **acredita** B **acredita** $A \overset{N_b}{\leftrightarrow} B$	(4)
A **acredita** B **controla** $A \overset{N_b}{\leftrightarrow} B$	(1)
A **acredita** $A \overset{N_b}{\leftrightarrow} B$	(13) (B3, 1, 4)

A recebe toda a fórmula (12). Aplica a regra de jurisdição (B3) nas suposições (1) e (4) e obtém a fórmula (13). Dessa forma, A possui N_b que será utilizado como parte da chave de sessão compartilhada (K_{ab}) entre ele e B.

Resultado: A acredita que possui parte da chave de sessão K_{ab}.

Mensagem 2:

B **recebeu** ($A \overset{N_a}{\leftrightarrow} B$, $\{\{N_c\}K_{ac}\}K_{ab}$)	(14)
B **recebeu** ($A \overset{N_a}{\leftrightarrow} B$)	(15) (B4, 14)
B **recebeu** ($\{\{N_c\}K_{ac}\}K_{ab}$)	(16) (B4, 14)
B **acredita** A **acredita** $A \overset{N_a}{\leftrightarrow} B$	(4)
B **acredita** A **controla** $A \overset{N_a}{\leftrightarrow} B$	(2)
B **acredita** $A \overset{N_a}{\leftrightarrow} B$	(17) (B3, 2, 4)

A recebe toda a fórmula (14). Aplicando a regra B4 obtém (15) e (16). Empregando a regra de jurisdição (B3) nas suposições (2) e (4) obtém a fórmula (17). Dessa forma, B possui N_a que será utilizado como parte da chave de sessão compartilhada (K_{ab}) entre ele e A.

Resultado: B acredita que possui parte da chave de sessão K_{ab}.

$K_{ab} = N_a \bullet N_b$

A **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$ (18) B **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$ (19)

Continuando a análise da segunda mensagem utilizando a fórmula (16):

B **recebeu** ($\{\{N_c\}K_{ac}\}K_{ab}$)	(16)
B **acredita** A **disse** $\{N_c\}K_{ac}$	(20) (B1, 16, 19)

B recebeu a fórmula (16) e como ele pode gerar a chave de sessão, a partir da combinação dos números aleatórios (N_a e N_b), então ele aplica a regra (B1) nas fórmulas (16) e (19) e chega na conclusão (20). Para a geração da chave de sessão é aplicada uma operação que está sendo representada pelo símbolo "•".

Resultado: B acredita que A há algum tempo disse $\{N_c\}K_{ac}$. Este valor será utilizado na autenticação de A.

Mensagem 3:

C **recebeu** $\{N_c\}K_{ac}$	(21)
C **acredita** A **disse** N_c	(22) (B1, 21, 7)
C **acredita** A **acredita** N_c	(23) (B2, 9, 22)

C recebeu toda a fórmula (21) e empregando a regra (B1) na suposição (7) e na fórmula (21) obtém (22). Utilizando a regra (B2) na suposição (9) e na fórmula (22), chega-se na fórmula (23).

Resultado: C autentica A.

Mensagem 4:

B **recebeu novo**$\{N_c\}K_{ac}$	(24)
B **acredita** C **acredita** (**novo**$\{N_c\}K_{ac}$)	(confiança no enlace cabeado)
B **acredita novo**$\{N_c\}K_{ac}$	(25) (B3, 10, 11)
B **acredita** A **disse** $\{N_c\}K_{ac}$	(20)
B **acredita** A **acredita** $\{N_c\}K_{ac}$	(26) (B2, 25, 20)

B recebe a fórmula (24). Aplica a regra (B3) nas suposições (10) e (11) e obtém a fórmula (25). Depois utiliza a regra (B2) nas fórmulas (25) e (20) para gerar a fórmula (26).

Resultado: B autentica A

Mensagem 5:

A **recebeu** {**novo**$\{N_c\}K_{ac}\}K_{ab}$	(27)

A **acredita** B **disse novo**$\{N_c\}K_{ac}$ (28) (B1, 27, 18)

A recebe a fórmula (27) pode aplicar a regra (B1) em (27) e (18) e conseguir (28).

Resultado: A recebe um novo valor de desafio que será utilizado na próxima comunicação. Como A recebeu uma mensagem de B cifrada com a chave de sessão, então ele acredita que B existe.

- Conclusão

Gerando $K_{ab} = N_a \bullet N_b$

Logo,

A **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$

B **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$

A **acredita** B **disse novo**$\{N_c\}K_c$

B **acredita** A **acredita** $\{N_c\}K_c$

C **acredita** A **acredita** N_c

De acordo com a análise da lógica BAN realizada neste trabalho, o protocolo consegue atingir os objetivos da autenticação do terminal móvel e de distribuição da chave de sessão. Porém, essas alegações somente são verdadeiras utilizando suposições duvidosas. Por exemplo, o protocolo realiza a troca de chave sem fazer uma autenticação entre os participantes.

Além disso, a distribuição das chaves é realizada empregando o protocolo Diffie-Hellman, que é reconhecido estar sujeito ao ataque do homem-no-meio, ou seja, um intruso pode agir entre os participantes legítimos iniciando duas trocas de chaves separadas, uma entre ele e a base e outra entre ele e o terminal móvel. A fraqueza na distribuição da chave abre a possibilidade para um intruso monitorar as

comunicações, obter o segredo compartilhado entre o móvel e a base e dessa forma, ter acesso aos serviços e às informações importantes.

Como no GSM, o protocolo CPDP acredita que a rede cabeada é segura, o que só deveria ser aceito, se houvesse algum protocolo de segurança implementado no *backbone*.

4.4. UMTS

Os sistemas de terceira geração (3G) tiveram o início de seu planejamento em 1992, quando a ITU percebeu que as comunicações móveis estavam crescendo rapidamente. Um grupo de estudos internacional previu que os telefones móveis concorreriam com as linhas fixas em dez anos, uma previsão que se tornou realidade em alguns países. Os sistemas de 3G começaram a funcionar em um projeto denominado FPLMTS (*Future Public Land Mobile Telecommunications System*) que tinha como objetivo criar um padrão único mundial (DORNAN, 2001).

Desde 1996, o padrão europeu W-CDMA[15] planejado ficou conhecido como UMTS. Seu desenvolvimento foi incentivado pelo UMTS Forum, um grupo do governo e do setor, encarregado de desenvolver um sucessor para o GSM.

Enquanto os sistemas 2G, como o GSM, continuam desempenhando um papel importante, o novo sistema 3G-UMTS já está sendo introduzido na Europa e na Ásia. Os sistemas 3G são essenciais para os serviços de Internet sem fio e quase sempre são considerados como futuro da comunicação móvel. Inicialmente, proporcionariam acesso permanente à Web, vídeo interativo e qualidade de voz semelhante à de um CD-player e não de um telefone celular, além de outros serviços.

Como nos sistemas 2G, a preocupação com a segurança é fundamental para o sistema UMTS e também deve satisfazer as exigências de sigilo dos dados, sigilo da identidade do assinante e autenticação do usuário. Enquanto estas características já são fornecidas nos sistemas existentes, elas precisam ser aprimoradas pela

[15] W-CDMA (*Wideband - Code Division Multiple Access*) – Sistema CDMA que utiliza canais de 5 GHz e é capaz de enviar chamadas sobre GSM.

incorporação de características adicionais do UMTS. A mais importante das novas características de segurança do UMTS é que o usuário também tem que autenticar a rede, impedindo que um intruso se passe por uma rede servidora (HORN e PRENEEL, 2000).

A arquitetura da rede UMTS é semelhante a utilizada pelo sistema de segunda geração GSM. Possui como entidades: terminal móvel, estação base, HLR/VLR, MSC, AC entre outros, com funcionalidades similares (FIG. 4.6). Cada terminal móvel possui um *chip* USIM (*User Services Identity Module*) que armazena a identidade do assinante, os algoritmos e as chaves de autenticação e ciframento, além de outras informações relacionadas ao assinante (BARBA, CRUSELLES e MELÚS, 1993).

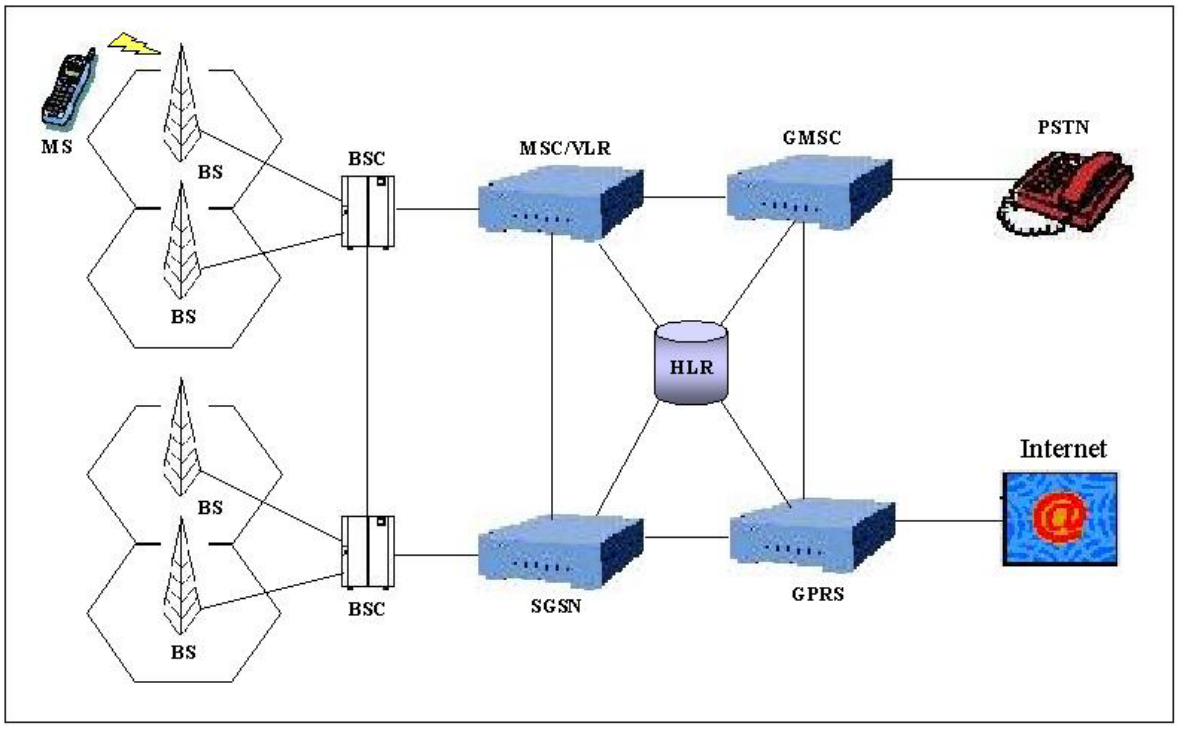

Fig. 4.6 – Arquitetura da Rede UMTS

Na FIG. 4.6 existem alguns componentes que não são encontrados no GSM:

- GMSC (*Gateway Mobile Switching Center*): é o comutador no ponto onde o UMTS é conectado à rede externa (como por exemplo, PSTN).
- GPRS (*General Packet Radio Service*): possui funcionalidade similar ao MSC/VLR mas é tipicamente utilizado como serviços de comutação de pacotes (Internet).

4.4.1. OBJETIVOS DO PROTOCOLO

As especificações para segurança 3G definem cinco categorias diferentes, dentre elas a segurança de acesso à rede, que tem o objetivo de proporcionar aos usuários acesso seguro. De acordo com suas definições, esta característica provê sigilo da identidade do usuário, autenticação dos usuários, sigilo dos dados, integridade dos dados e identificação do terminal móvel.

- sigilo da identidade do assinante: é realizado pelo uso de identidades temporárias (TMUI – *Temporary Mobile User Identity*) com validade local (como no GSM). O gerenciamento da TMUI ocorre durante a atualização da localização da mesma maneira que no GSM. Evita-se transmitir a identidade legítima (IMUI – *International Mobile User Identity*) sobre a interface aérea em texto claro;
- autenticação do usuário (autenticação e distribuição da chave) é realizada através da autenticação mútua entre o usuário e a rede, usando a chave secreta, conhecida somente pelo usuário, USIM, e a AC. Além disso, o usuário e o HLR mantém os respectivos contadores SEQ_a e SEQ_b para apoiar a autenticação. O UMTS utiliza um mecanismo de desafio-resposta semelhante ao do sistema GSM (para máxima compatibilidade);
- sigilo dos dados do assinante: é realizado através de algoritmos de ciframento entre o móvel e a rede servidora. É estabelecida uma chave de sessão secreta como parte do processo de autenticação;

- integridade dos dados: esta é uma das novas características de segurança incluída nos sistemas 3G. O algoritmo de integridade do UMTS junto com uma chave de integridade é utilizado para prover integridade dos dados. A chave de integridade também é estabelecida durante o processo de autenticação e o algoritmo de integridade é negociado entre as partes, que depois poderá verificar a integridade das informações recebidas;
- identificação do terminal móvel: é feito através do IMEI que identifica exclusivamente um equipamento móvel (semelhante ao sistema de GSM).

4.4.2. FLUXO DE MENSAGENS

O protocolo de autenticação proposto é baseado no sistema criptográfico de chave simétrica. Ela possui somente três mensagens trocadas entre o móvel, representado no fluxo por A, e a rede servidora, representada por B. Este protocolo combina o fornecimento do sigilo da identidade do usuário, a autenticação da entidade e a distribuição da chave de sessão num único mecanismo (FIG. 4.7).

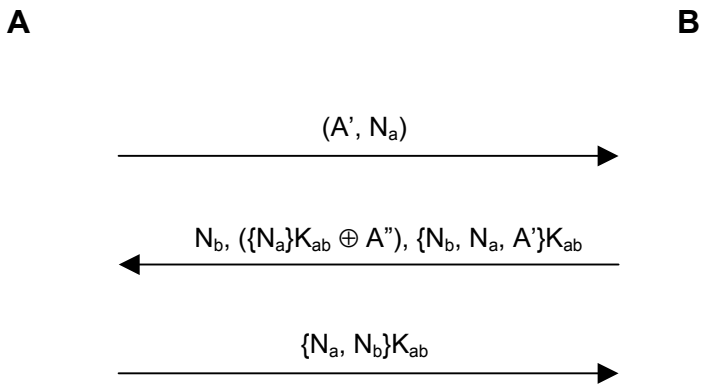

FIG. 4.7 – Protocolo de Autenticação do UMTS

1º Passo: O móvel A gera um número aleatório (N_a) e envia-o para a rede operadora B, juntamente com a identidade temporária (A').

2º Passo: B gera um outro número aleatório (N_b) e calcula: {N_b, N_a, A'}K_{ab}, {N_a}K_{ab} e a nova identidade temporária (A"). B envia tudo para A.

A recebe a mensagem e decifra $\{N_b, N_a, A'\}$ com a chave secreta compartilhada com B e obtém o número aleatório N_b que será verificado com o N_b enviado em texto em claro. Verifica se na mensagem contém o N_a enviado na primeira mensagem, e dessa forma, A autentica a rede operadora, B. A também obtém a nova identidade temporária.

3º Passo: A calcula: $\{N_a, N_b\}K_{ab}$. Então envia para B.

B recebe, decifra a mensagem e verifica se o número aleatório (N_b) recebido é igual ao que foi emitido na segunda mensagem. Se for, então o móvel é autenticado e dessa forma, B e A podem calcular a chave de sessão, utilizando A um algoritmo para geração de chave, onde as entradas são N_a, N_b, A" e cifradas com a chave secreta K_{ab}.

4.4.3. ANÁLISE FORMAL

- Protocolo

M1: $A \rightarrow B$ A', N_a

M2: $B \rightarrow A$ $N_b, (\{N_a\}K_{ab} \oplus A"), \{N_a, N_b, A'\}K_{ab}$

M3: $A \rightarrow B$ $\{N_a, N_b\}K_{ab}$

- Protocolo Idealizado

M1 $A \rightarrow B$ N_a

M2 $B \rightarrow A$ N_b, **novo**$(\{N_a\}K_{ab} \oplus A"), \{N_a, N_b\}K_{ab}$

M3 $A \rightarrow B$ $\{N_a, N_b\}K_{ab}$

- Suposições

1. A **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$
2. B **acredita** $A \overset{K_{ab}}{\leftrightarrow} B$

3. B **acredita** A **disse** N_a

4. A **acredita** B **disse** N_b

5. B **acredita novo**(N_b)

6. A **acredita novo**(N_a)

7. A **acredita** B **disse novo**($\{N_a\}K_{ab} \oplus$ A")

8. A **acredita novo**($\{N_a\}K_{ab} \oplus$ A")

- Prova

Mensagem 1:

B **recebeu** N_a	(9)
B **acredita** A **disse** N_a	(10) (suposição 3)

Resultado: B obtém N_a.

Mensagem 2:

A **recebeu** N_b, **novo**($\{N_a\}K_{ab} \oplus$ A"), $\{N_a, N_b\}K_{ab}$	(11)
A **recebeu** N_b	(12) (B6, 11)
A **recebeu novo**($\{N_a\}K_{ab} \oplus$ A")	(13) (B6, 11)
A **recebeu** $\{N_a, N_b\}K_{ab}$	(14) (B6, 11)
A **acredita** B **disse** $\{N_a, N_b\}$	(15) (B1, 14, 1)
A **acredita** B **disse** N_a	(16) (B5, 15)
A **acredita** B **acredita** N_a	(17) (B2, 16, 6)
A **acredita** B **disse** N_b	(18) (B5, 15)
A **acredita** B **acredita novo**($\{N_a\}K_{ab} \oplus$ A")	(19) (B2, 7, 8)

A recebe a fórmula (11) e aplica a regra (B6) e encontra as fórmulas (12), (13) e (14). Utiliza a regra (B1) em (14) e (1) e obtém a fórmula (15), depois emprega a regra (B2) em (16) e na suposição (6) e consegue (17).

Resultado: A autentica B.

Depois de autenticar B, A pode gerar a chave de sessão utilizando a nova identidade temporária A" e os números aleatórios N_a e N_b (18). A identidade temporária é extraída da fórmula (19) calculando a operação inversa XOR, com a entrada $\{N_a\}K_{ab}$. Essa mesma operação é executada por B.

Mensagem 3:

B **recebeu** $\{N_a, N_b\}K_{ab}$	(20)	
B **acredita** A **disse** $\{N_a, N_b\}$	(21)	(B1, 20, 2)
B **acredita** A **acredita** N_b	(22)	(B2, 21, 5)

B recebe a fórmula (20). Aplica a regra de significado da mensagem (B1) na suposição (2) e na fórmula (20) e obtém (21). Depois utiliza a regra de verificação do identificador (B2) em (21) e em (5) e consegue (22).

Resultado: B autentica A.

- Conclusão

A **acredita** B **acredita** N_a	A autentica B
B **acredita** A **acredita** N_b	B autentica A

A e B calculam a chave de sessão.

A análise mostra que o protocolo de autenticação UMTS alcança os objetivos mostrados em 4.4.1, ou seja, a autenticação mútua, a distribuição da chave de

sessão e o sigilo da identidade e dos dados do assinante. Porém, se um intruso conseguir obter a chave secreta K_{ab}, poderá se passar por um assinante legítimo e ter acesso a todas as informações.

4.5. CONSIDERAÇÕES FINAIS

Neste trabalho foram realizadas as avaliações de três protocolos do ambiente de comunicação celular: GSM, CDPD e UMTS. De acordo com a análise, chega-se a conclusão que é importante aplicar um método formal que verifique os requisitos desejados pelos protocolos. Como visto, muitas suposições duvidosas devem ser levadas em consideração para que os objetivos dos protocolos sejam atingidos.

O protocolo de autenticação do GSM é simples e é esperado fornecer o sigilo da identidade do usuário e dos dados, a autenticação do assinante e a distribuição da chave. Apesar de, aparentemente, esses objetivos serem alcançados, a principal conclusão da análise é que o móvel não acredita que a chave de sessão seja satisfatória, já que o valor utilizado para gerar a chave pode ter vindo de um intruso.

O protocolo de autenticação do CDPD já inicia com problemas. Além dos participantes não se autenticarem antes de trocarem informações importantes (valores que serão usados no cálculo da chave), a chave de sessão é gerada empregando o esquema de troca de chaves Diffie-Hellman. Se um intruso agir entre os participantes poderá criar duas chaves de sessão, uma entre ele e o móvel e outra entre ele e a rede e dessa forma, obter todas as informações. O intruso poderá ler, apagar e modificar todas as mensagens enviadas pelos participantes.

Outro problema é com a confiança que esses dois protocolos possuem em relação à rede cabeada. Todas as mensagens são enviadas em texto em claro e essas informações podem ser úteis a um intruso.

E, finalmente, com o protocolo de autenticação UMTS, a análise mostrou que os objetivos foram alcançados. Como foi mencionado no terceiro capítulo, a lógica BAN verifica a veracidade dos objetivos propostos pelos desenvolvedores do protocolo, porém não fornece uma prova de segurança. É claro que utilizando o método podem ser tiradas conclusões importantes. Por exemplo, considerando uma

suposição duvidosa, pode-se dizer que um intruso consegue obter informações importantes, tais como a chave de sessão ou a identidade do usuário e utilizá-las, indefinidamente, para se passar por um usuário legítimo e ter acesso às informações ou até mesmo realizar chamadas gratuitas.

Para complementar a análise e confirmar a segurança do protocolo é importante que seja empregado algum método de criptoanálise e, dessa forma, verificar a força do algoritmo utilizado no protocolo, analisar os ataques que os protocolos ou os algoritmos estão sujeitos e se há a possibilidade de um intruso obter alguma chave.

O protocolo de autenticação do UMTS é bastante reduzido, são somente três mensagens enviadas, que servirão para a autenticação mútua e para a geração da chave. Um intruso pode, por exemplo, utilizar o ataque por reflexão, abrir sessões diversas (não são utilizados *timestamps*) conseguir obter a identidade temporária do móvel e a chave de sessão.

5. CONCLUSÕES E TRABALHOS FUTUROS

5.1. CONCLUSÃO

A maior contribuição deste trabalho foi mostrar para as áreas acadêmica e comercial que é importante o emprego de um método formal no planejamento e na verificação de protocolos criptográficos. Mesmo que aparentemente o protocolo funcione, uma avaliação mais detalhada consegue revelar se os objetivos de segurança propostos são obtidos. Além disso, é importante salientar que o custo-benefício em utilizar uma dessas abordagens, antes de publicar o protocolo, é melhor do que ter que fazer modificações posteriores. É, obviamente, mais barato usar os métodos no planejamento do protocolo do que fazer o seu replanejamento.

Nesse trabalho, foi realizada uma comparação entre as lógicas BAN (BURROWS, ABADI e NEEDHAM, 1990) e GNY (GONG, NEEDHAM e YAHALOM, 1990) utilizando o protocolo de distribuição de chaves Needham-Schroeder (SCHNEIER, 1996), que apesar de ter sido analisado nos respectivos artigos, não havia sido avaliado pelas duas abordagens ao mesmo tempo e nem explicado de forma detalhada como mostrado.

A lógica BAN foi a pioneira em empregar um método formal baseado em lógica modal para idealizar e analisar protocolos criptográficos, principalmente os de autenticação e distribuição de chaves. A análise é baseada num conjunto de regras que aplicadas, podem deduzir as crenças e o conhecimento dos participantes do protocolo.

A lógica GNY é uma das extensões da lógica BAN de maior sucesso que também utiliza o conceito de crença entre os participantes. Introduziu novas definições, como as de reconhecimento, de posse e a expressão “não-originada-aqui” na qual evita o reenvio de mensagens antigas. Porém, por conter uma grande quantidade de postulados lógicos (são mais de cinqüenta) e ter que considerar muitas regras em cada fase do protocolo, é muito mais complexa na compeensão e sua aplicação torna-se muito complicada.

Um dos problemas encontrados com as lógicas são com as suposições realizadas. Deve-se tomar cuidado na hora de elaborá-las, já que são através delas que as provas são obtidas. Suposições erradas, conseqüentemente irão gerar conclusões falsas. Em (BOYD e MAO, 1994) são mostradas algumas das limitações da lógica BAN. Apesar das críticas, é importante ressaltar que a lógica BAN encontrou erros e redundâncias em vários protocolos (BURROWS, ABADI e NEEDHAM, 1990) e ainda é utilizada na validação de alguns trabalhos, como por exemplo pode-se citar (MYRVANG, 2000).

De acordo com a comparação entre as lógicas, observou-se que a abordagem BAN é mais simples e fácil de aplicar, obtendo, praticamente, os mesmos resultados (ver TAB. 3.1 – Comparação das Conclusões entre as Lógicas BAN e GNY – no terceiro capítulo). Entretanto, um dos problemas com os métodos baseados em lógica modal são as suposições que devem ser feitas de maneira cautelosa. Um analista precisa tomar cuidado para não fazer uma análise equivocada do protocolo. Ele deve observar se as suposições são corretas, pois a partir delas é que serão tiradas as conclusões da avaliação.

No quarto capítulo foi sugerida e empregada uma notação mais intuitiva para a análise dos protocolos de autenticação do ambiente celular, substituindo alguns dos símbolos utilizados na lógica BAN por palavras, destacadas no texto em negrito, que expressam seus signifcados, facilitando a compreensão da lógica. Por exemplo, a palavra ”**novo**” representa o símbolo “**#**”.

Outra contribuição foi a avaliação dos protocolos de autenticação do ambiente celular, onde foi realizada a validação do trabalho de (Godfrey, 1995), que utilizou a lógica BAN para analisar os protocolos de autenticação do GSM e CDPD. Porém, nesta dissertação (quarto capítulo) foi mostrada de forma detalhada a análise e foram utilizados outros postulados e outras suposições obtendo os mesmos resultados. Além disso, não havia sido realizada a análise do protocolo de autenticação do UMTS e uma comparação entre os três protocolos (GSM, CDPD e UMTS). De acordo com a análise, observou-se que muitas suposições duvidosas devem ser levadas em consideração para que os objetivos dos protocolos fossem atingidos.

O protocolo de autenticação do GSM possui como metas: fornecer o sigilo dos dados e da identidade do móvel, a autenticação do assinante e a distribuição da

chave de sessão entre os participantes. Apesar de, aparentemente, esses objetivos serem alcançados, a principal conclusão da análise é que o móvel não acredita que a chave seja satisfatória, já que o valor utilizado para gerá-la pode ter vindo de um intruso.

No protocolo de autenticação do CDPD, os participantes iniciam a comunicação trocando informações importantes (valores que serão usados no cálculo da chave) sem se autenticarem. Além disso, a chave de sessão é gerada empregando o esquema de troca de chaves Diffie-Hellman. Se um intruso agir entre os participantes poderá criar duas chaves de sessão, uma entre ele e o móvel e outra entre ele e a rede, podendo, dessa forma, ler, apagar e modificar todas as mensagens enviadas.

Outro problema é na crença que esses dois protocolos possuem em relação à rede cabeada. Todas as mensagens enviadas entre a estação base e a rede estão em texto em claro e essas informações podem ser de especial interesse a um intruso.

Finalmente, a análise realizada do protocolo de autenticação UMTS mostra que os objetivos foram alcançados. Contudo é importante que seja empregado algum tipo de criptoanálise para garantir a segurança do mesmo. É importante ressaltar que a lógica é considerada como um dos passos que devem ser executados para verificar se existe alguma fraqueza no protocolo que pode ser aproveitada por um intruso.

5.2. TRABALHOS FUTUROS

Os métodos formais, durante muito tempo, foram empregados na análise de protocolos de comunicação. No final dos anos setenta e início de oitenta foram desenvolvidos alguns dos trabalhos promissores na análise de protocolos criptográficos. Mas em geral, o interesse pela aplicação de métodos formais nesses protocolos não foi difundido até o início da década de noventa, quando vários pesquisadores encontraram falhas de segurança usando técnicas de análise formal, como é o caso do artigo de (BURROWS, ABADI e NEEDHAM, 1990).

Esses métodos podem ser utilizados em várias fases do planejamento, desde a especificação e construção até a verificação. Todavia, a maioria dos trabalhos concentram-se na verificação formal de protocolos, e em particular, na aplicação de lógicas modais de conhecimento e crença.

Como sugestão de trabalhos futuros, é propor uma linguagem de especificação universal para ser utilizada num analisador automático, como NRL (MEADOWS, 2000) e o AAPA2 (BRACKIN, 2000). Ainda existem poucos trabalhos nesta área, e os que existem, ainda possuem limitações (FREIRE, 2000) e (BUTTYÁN, 1999).

Pode ser estudado também métodos formais específicos para protocolos de segurança que já levem em consideração as características das redes sem fio. Com a crescente demanda, por exemplo, da Internet móvel, é importante que sejam elaborados protocolos e que sejam realizadas verificações.

Finalmente é recomendado que sejam feitas avaliações para o ambiente Ad hoc e para redes locais sem fio (WLAN). Os poucos protocolos criptográficos utilizados nestas áreas foram desenvolvidos para as redes cabeadas e adaptados para estes ambientes. Além disso, não foram encontradas análises desses protocolos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ANATEL. **Agência Nacional de Telecomunicações.** Disponível em http://www.anatel.gov.br. 2002.

ASOKAN, N. **Security Issues in Mobile Computing**. Disponível em http://www.semper.org/sirene/people/asokan/research/proposal.ps.gz .Abril 1995.

AYDOS, M, YANIK, T. e KOÇ, Ç. K. **An High-Speed ECC-based Wireless Authentication Protocol on an ARM Microprocessor**. 16th Annual Computer Security Applications Conference. Nova Orleans. Dezembro 2000.

AZIZ, Ashar e DIFFIE, Whitfield. **Privacy and Authentication for Wireless Local Area Networks**. IEEE Personal Communications. pp. 25-31.1994.

BARBA, A., CRUSELLES, E. e MELÚS, J. L. **The Customer Premises Network (CPN) in the Universal Mobile Telecommunication System – Security Aspects**. 4º WINLAB Workshop on 3rd Generation WIN. Nova Jersey. Outubro 1993.

BASYOUNI, A. M e TAVARES, S. E. **Public Key versus Private Key in Wireless Authentication Protocols**. Queen's University, 1996. Disponível em www.ece.queensu.ca/department/ reports/report97/grad.pdf

BASYOUNI, Ayda M. **Analysis of Wireless Cryptographic Protocols**. Dissertação de Mestrado em Engenharia de Sistemas. Queen's University, Canadá. Agosto de 1997. Disponível em http://adonis.ee.queensu.ca.8000/pn/.

BEHEN, Jonannes. **Security first in Europe's mobile communications**. Siemens AG. Telcom Report International vol.17, nº 1. 1994

BELLER, Michael J., CHANG, Li-Fung e YACOBI, Yacov. **Privacy and Authentication on a Portable Communications Systems**. IEEE Journal on Selected Areas in Communications, vol. 11, nº 6, pp. 821-828. Agosto 1993.

BOYD, Colin e MAO, Wenbo. **Limitations of Logical Analysis of Cryptographic Protocols**. Advances in Cryptology. Eurocrypt'93. pp. 240-247. 1994. Disponível em http://citeseer.nj.nec.com/boyd93limitations.html

BRACKIN, Stephen H. **Automatically Detecting Most Vulnerabilities in Cryptographic Protocols**. Publicado como ATR99031, Arca Systems, Inc. Junho 1999. Disponível em http://www.arca.com/proj-papers/informal.html.

BRACKIN, Stephen H. **User's Manual for the Automatic Authentication Protocol Analyzer (AAPA2)**. 2ª versão. Arca Systems. 2000. Disponível em www.arca.com/projects/docs/brackin/quarter8.pdf

BRANCHAUD, Marc. **A Survey of Public Key Infrastructures**. 1997. 84 p. Dissertação (Mestrado em Ciência da Computação) – Universidade de Montreal, 1997. Disponível em cnscenter.future.co.kr/security/pki-more.html

BRASIL. Decreto Lei nº 3.587, de 5 de setembro de 2000. **Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov**. Diário Oficial da República Federativa do Brasil. Brasília, 5 de setembro de 2000.

BURROWS, M., ABADI, M. e NEEDHAM, R. **A logic of authentication**. ACM Transactions on Computer Systems, vol. 8, pp. 18-36. 1990.

BUTTYÁN, Levente. **Formal methods in the design of cryptographic protocols**. Disponível em http://citeseer.nj.nec.com/context/1960161/0. Technical Report SSC/. Novembro 1999.

CHANG, C.-C, HUANG, P.-C e LEE, W.-B. **Conference key Distribution schemes for portable communication systems**. Computer Communications, 22, pp. 1160-1164. 1999.

CLARK, J. e JACOB, J. **A Survey of Authentication Protocol Literature: Version 1.0**. Uma biblioteca de protocolos analisados na literatura, atualizada continuamente, disponível em www.cs.york.ac.uk/~jac/. 1998.

DAEMEN, J. e RIJMEN, R.V. **The Advanced Encryption Standard (AES)**. Dr. Dobb's Journal, vol. 26 nº 3, pp. 137-139. Março 2001.

DENNING, Dorothy E. e SACCO, Giovanni Maria. **Timestamps in Key Distribution Protocols**. Communications of the ACM, vol. 24, nº 8 pp. 533-536. Agosto 1981.

DENNING, Dorothy. **Cryptography and Data Security**. Addison-Wesley Publishing Co., Inc. 1982.

DIFFIE, Whitfield e HELLMAN, Martin E. **New Directions in Cryptography**. IEEE Transactions on Information Theory, vol IT-22, nº 6. Novembro 1976.

DIFFIE, Whitfield e HELLMAN, Martin E. **Privacy and Authentication: An Introduction to Cryptography**. Proceedings of the IEEE, vol. 67, nº 3. Março 1979.

DORNAN, Andy. **The Essential Guide to Wireless Communication**. ISBN 0-13-031716-0. 304 p. Prentice Hall PTR. 2001.

ELLISON, Carl e SCHNEIER, Bruce. **Ten Risks of PKI: what you're not being told about Public Key Infrastructure**. Computer Security Journal. Volume XVI, nº 1, 2000.

FRANKEL, Yair et. al. **Security Issues in a CDPD Wireless Network**. IEEE Personal Communications, pp. 16-27. Agosto1995.

FREIRE, Clóvis. **Identificação da Necessidade de Especificação Formal no Projeto de Protocolos Criptográficos.** Simpósio Segurança em Informática. São José dos Campos: CTA/ITA/IEC, 2000.

GALBRAITH, Steven. **Elliptic Curve Cryptosystems Project First Meeting**. Janeiro 1997. Disponível em http://www.cs.bris.ac.uk/Research/CryptographySecurity/biblio.html

GERCK, Ed. **Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP. Julho 2000**. Disponível em www.mcg.org.br/certover.pdf

GODFREY, James. **A Comparison of Security Protocols in a Wireless Network Environment**. Dissertação de Mestrado. Universidade de Waterloo. Canadá – 1995. Disponível em citeseer.nj.nec.com/did/40794

GONG, Li, NEEDHAM, Roger e YAHALOM, Raphael. **Reasoning about Belief in Cryptographic Protocols**. Proceedings of the IEEE. Simpósio de Segurança e Privacidade. Califórnia. Maio de 1990, p. 234-248.

GRITZALIS, S., SPINELLIS, D. e GEORGIADIS, P. **Security protocols over open networks and distributed systems: formal methods for their analysis, design and verification**. Computer Communications, vol. 22, nº 8, pp. 697-709. Maio 1999.

HORN, Günther e PRENEEL, Bart. **Authentication and Payment in Future Mobile Systems**. ESORICS'98 – LNCS 1485, pp. 277-293. 1998. Disponível em http://citeseer.nj.nec.com/82814.html

HORN, Günther e PRENEEL, Bart. **Authentication and Payment in Future Mobile Systems**. Journal of Computer Security, vol.8 n. 2/3. 2000. Disponível em http://www.informatik.uni-trier.de/~ley/db/journals/jcs/jcs8.html

JOSEPH, Anthony D. **Privacy and Security in Wireless Networks**. Disponível em http://www.cs.berkeley.edu/~adj/cs294-1.f00/L8.pdf . Outubro 2000.

KEMMERER, R. **Analyzing encryption protocols using formal verification techniques**. IEEE Journal on Selected Areas in Communications, vol. 7, nº 4, pp. 448-457. Outubro 1989.

KEMMERER, R., MEADOWS, Catherine e MILLEN, J. **Three systems for cryptographic protocol analysis**. Journal of Cryptology, vol.7 pp. 79-130. 1994.

KYNTAJA, Timo. **A Logic of Authentication by Burrows, Abadi and Needham**. Disponível em http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/ban.html. 1995.

LEE, Wei-Bin e CHANG, Chin-Chen. **Authenticity of Public Keys in Asymmetric Cryptosystems**. Computer Communications 21, pp. 195-198. 1998.

LIN, Hung-Yu e HARN, Lein. **Authentication Protocols for Personal Communication Systems**. Proceedings of ACM SIGCOMM'95, pp. 256-261, August 1995. Disponível em http://citeseer.nj.nec.com/lin95authentication.html

LIN, Hung-Yu, HARN, Lein e KUMAR, Vijay. **Authentication Protocols in Wireless Communications**. ICAUTO'95. 1995. Disponível em cs.engr.uky.edu/~singhal/CS685-papers/ authentication-protocols-in-wireless.pdf

LIN, Hung-Yu e HARN, Lein. **Authentication Protocols with Non-Repudiation Services in Personal Communications Systems**. Disponível em http://www.cstp.umkc.edu/~harn/paper14/paper14.htm. 1999

LÓPEZ, Julio e DAHAB, Ricardo. **Performance of Elliptic Curve Cryptosystems**. Relatório Técnico IC-00-08. Unicamp. São Paulo. Maio de 2000. Disponível em citeseer.nj.nec.com/lopez00performance.html

LOWE, Gavin. **A Hierarchy of Authentication Specifications**. Proceedings of 10th IEEE Computer Security Foundations Workshop. 1997.

LOWE, Gavin. **An Attack on the Needham-Schroeder Public Key Authentication Protocol**. Information Processing Letters, vol. 56, nº 3, pp. 131-133. 1995.

LOWE, Gavin. **Casper: a Compiler for the Analysis of Security Protocols**. Proceedings of 10th IEEE Computer Security Foundations Workshop. 1997.

MATHURIA, Anish, NAINI, Reihaneh Safavi e NICKOLAS, Peter. **Some Remarks on the Logic of Gong, Needham and Yahalom**. Proceedings of the International Computer Symposium. 1994. Taiwan. vol. 1 p. 303-308

MEADOWS, Catherine. **Formal verification of cryptographic protocols: A survey**. ASIACRYPT'94: Advances in Cryptology – International Conference on the Theory and Application of Cryptology – pp 133-150. 1995. Disponível em http://citeseer.nj.nec.com/134868.html

MEADOWS, Catherine. **Open Issues in Formal Methods for Cryptographic Protocol Analysis**. DISCEX 2000: Proceedings of the DARPA Information Survivability Conference and Exposition, v. 1, p. 237-250. IEEE Computer Society Press. Janeiro 2000.

MEHROTRA, Asha e GOLDING, Leonard S. **Mobility and Security Management in the GSM System and Some Proposed Future Improvements**. Proceedings of the IEEE, vol. 86, nº 7. Julho 1998.

MITCHELL, Christopher, WALKER, Michael e RUSH, David. **CCITT/ISO Standards for Secure Message Handling**. IEEE Journal on Selected Areas in Communications. vol.7, nº 4, Maio de 1999.

MOLVA, Refik, SAMFAT, Didier e TSUDIK, Gene. **Authentication of Mobile Users**. IEEE Network, vol. 8, nº 2, pp 26-34. Março/Abril 1994.

MONNIAUX, David. **Decision Procedures for the Analysis of Cryptographic Protocols by Logics of Belief**. In 12th Computer Security Foundations Workshop. 1999. Disponível em http://www.di.ens.fr/~monniaux/biblio/Monniaux_CSFW12.pdf

MOULY, Michel e PAUTET, Marie-Bernadette. **The GSM System for Mobile Communications**. M. Mouly e M.-B. Pautet Eds, 1992. ISBN 2-9507190-0-7

MOURA, Giedre. **Tão Longe, tão perto**. Network Computing Brasil, São Paulo, ano 3, n. 30, p. 36-44, agosto 2001. Disponível em www.networkcomputing.com.br

MYRVANG, Per Harald. **An Infrastructure for Authentication, Authorization and Delegation**. 2000. Tese (Doutorado em Ciência da Computação) – Universidade de Troms∅, Faculdade de Ciência, Maio de 2000. Disponível em www.cs.uit.no/studier/gradseksamen/myrvang.html

NEEDHAM, R. M. e SCHROEDER, M. D. **Using Encryption for Authentication in Large Networks of Computers**. Communications of the ACM, 21 (12) p. 993-999, Dezembro 1978.

OORSCHOT, Paul C. Van, VANSTONE, Scott A. e MENEZES, Alfred. **Handbook of Applied Cryptography**. CRC Press. 1996.

PARK, Chang-Seop. **On Certificate-Based Security Protocols for Wireless Mobile Communication Systems**. IEEE Network – Setembro/Outubro 1997.

PARK, Kun Il. **Personal and Wireless Communications: Digital Technology and Standards**. Estados Unidos: Kluwer Academic Publishers, 1996. 230 p.

PATIYOOT, Danai e SHEPHERD, S.J. **Cryptographic Security Techniques for Wireless Networks**. ACM Operating Systems Review, vol. 33, nº 2, pp 36-50. Abril 1999.

PATIYOOT, Danai e SHEPHERD, S.J. **Techniques for Authentication Protocols and Key Distribution on Wireless ATM Networks**. ACM Operating Systems Review, vol. 32, nº 4, pp. 25-32. Outubro 1998. Disponível em http://www.ssh.fi/tech/crypto/intro.html.

RAMASAMI, Vijaya Chandran. **Security, Authentication and Access Control for Mobile Communications**. Disponível em http://www.ittc.ukans.edu/~rvc/wireless/overall.pdf. 2000.

RAPPAPORT, Theodore S. **Wireless Communications – Principles and Practice**. Prentice Hall PTR. 1996

RUBIN, Aviel D. e HONEYMAN, Peter. **Formal Methods for the Analysis of Authentication Protocols**. Technical Report CITI TR 93-7. Outubro 1993. Disponível em www.citi.umich.edu/u/honey/papers.html

SALLES, Ronaldo Moreira. **Protocolos de Múltiplo Acesso para Redes Sem Fio**. Dissertação (Mestrado). Instituto Militar de Engenharia, p. 118. Rio de Janeiro – 1998

SCHNEIER, Bruce. **Applied Cryptography – Protocols, Algorithms and Source Code in C** – 2ª Edição. John Wiley & Sons, Inc. 1996. ISBN 0-471-12845-7.

SEBERRY, Jennifer e PIEPRZYK, Josef. Cryptography: **An Introduction to Computer Security**. Advances in Computer Science Series – Prentice Hall. 1994. ISBN 0-13-194986-1.

SIDHU, D. **Authentication protocols for computer networks**. Computer Networks ad ISDN Systems. vol.11, págs. 297-310. 1986.

SOARES, L. F. G., LEMOS, G e COLCHER, S. **Redes de Computadores: das LANs, MANs e WANs às redes ATM**. 2ª edição. Rio de Janeiro : Campus, 1995. 705 p. ISBN 85-7001-954-8.

STINSON, Douglas. **Cryptography: Theory and Practice**. CRC Press. 1995.

SYVERSON, Paul e CERVESATO, Iliano. **The Logic of Authentication Protocols**. FOSAD´00: 1st International School on Foundations of Security Analysis and Design. Itália. Setembro 2000.

TANENBAUM, Andrew S. **Computer Networks**. 3ª edição. New Jersey: Prentice Hall PTR, 1996. ISBN 0-13-349945-6.

VARBusiness Brasil. **TECNOLOGIA: o futuro é wireless**. Ano 1, n. 7, p. 32-36, outubro 2000. Disponível em www.varbusiness.com.br.

VARADHARAJAN, V. **Use a formal description technique in the specification of authentication protocols**. Computer Standards and Interfaces, vol. 9, pp. 203-215. 1990.

VARADHARAJAN, V. **Verification of network security protocols**. Computers and Security, vol. 8, págs. 693-708. Elsevier Advanced Technology. 1989.

YACOUB, Michel Daoud**. Foundations of Mobile Radio Engineering**. CRC Press, Inc., 2000 Corporate Blvd. P. 481. ISBN 0-8493-8677-2. 1993.