Análise Formal de Protocolos de Segurança para Redes Celulares

Myrna C. M. dos Santos
Instituto Militar de Engenharia - IME
myrnasantos@bol.com.br

José A. M. Xexéo
Instituto Militar de Engenharia – IME
xexeo@bennett.br

José F. de Rezende
GTA/COPPE/UFRJ
rezende@gta.ufrj.br

RESUMO

O crescimento extraordinário 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. Para garantir a segurança vários protocolos foram desenvolvidos. Esses protocolos utilizam técnicas de criptografia para alcançarem seus objetivos, tais como, sigilo, autenticação, integridade dos dados e não-repúdio, entretanto, esses protocolos criptográficos estão sujeitos a erros no desenvolvimento, tornando-os vulneráveis a ataques. Foram criados então, métodos formais que têm a função de analisar e verificar se as metas propostas pelos autores dos protocolos foram alcançadas. Este trabalho tem como finalidade mostrar a importância do emprego de métodos formais nos protocolos criptográficos, e para isso apresenta 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.

Palavras-chave: protocolos de autenticação, análise formal, distribuição de chaves, lógica BAN, redes celulares.

1. INTRODUÇÃO

O setor de comunicaçao sem fio é um dos setores de maior crescimento da tecnologia da informação. No Brasil, a Agência Nacional de Telecomunicações espera que em 2005 para cada 100 habitantes existam 32,6 celulares.

Atualmente, serviços realizados pela Internet como compras *on-line* e até mesmo transações bancárias podem ser feitos por alguns aparelhos celulares (*m-commerce*).

Em contrapartida há um aumento no número de crimes relacionados às telecomunicações. Por isso, empresas, áreas governamentais, acadêmicas e militares sentem-se vulneráveis quando a segurança das informações é ignorada.

Nas redes de comunicação as mensagens são trocadas entre as entidades e como o ambiente móvel é mais suscetível a ataques, já que usam o ar como meio de transmissão, qualquer um com um receptor apropriado pode interceptar as mensagens sem ser detectado. Expondo informações importantes, como senhas e documentos, a não ser que estejam protegidas de alguma forma.

Para garantir a segurança das informações foram desenvolvidos vários protocolos que utilizam técnicas de criptografia para a implementação de serviços de segurança tais como sigilo do conteúdo das mensagens e da identidade do usuário/entidade, autenticação dos participantes na comunicação, integridade dos dados e não-repúdio (SCHNEIER, 1996).

Porém, se o protocolo criptográfico não for projetado corretamente proporcionará a um intruso a oportunidade de ataque por meio dos seguintes processos: substituição, exclusão, alteração ou criação de mensagens, ou pelo ataque aos algoritmos criptográficos utilizados. Por isso, vários métodos formais têm sido propostos a fim de analisar e projetar protocolos criptográficos.

O principal objetivo deste trabalho é mostrar para a área acadêmica e comercial a importância do emprego de métodos formais no desenvolvimento de protocolos criptográficos. A demanda crescente do setor sem fio, motivou a realização da análise de alguns dos principais protocolos de autenticação do ambiente celular: GSM, CDPD e UMTS.

O trabalho está dividido da seguinte forma: a seção 2 apresenta os serviços de segurança que um protocolo criptográfico para o ambiente sem fio deve fornecer; na seção 3 são mencionados os tipos de métodos formais encontrados na literatura; na seção 4 é realizada a análise formal de três protocolos de autenticação do ambiente celular (GSM, CDPD e UMTS). E, finalmente, na seção 5 são feitas as considerações finais.

2. SERVIÇOS DE SEGURANÇA

Os principais serviços de segurança que um protocolo criptográfico deve fornecer ao ambiente móvel, observadas as limitações desse ambiente, são:

- autenticação mútua: autenticação é o processo que confirma a identidade do usuário/entidade. Este serviço é realizado para que um intruso não se passe, por exemplo, por uma estação base legítima e obtenha informações importantes;
- estabelecimento da chave de sessão: durante o processo de autenticação, um segredo comum, denominado chave, deve ser negociado entre as partes.

A chave é utilizada para cifrar e decifrar as informações que serão transmitidas posteriormente ao processo de autenticação. É importante que esta chave seja trocada a cada sessão, evitando que um intruso utilize uma chave antiga;

- sigilo: é a condição na qual dados sensíveis são mantidos secretos e divulgados apenas às partes autorizadas. As mensagens, a identidade do usuário e a sua localização são consideradas importantes e não devem ficar expostas. Para garantir o sigilo das mensagens é realizado o ciframento de seu conteúdo usando a chave de sessão estabelecida. Para garantir o sigilo da identidade e da localização do assinante, alguns protocolos utilizam uma identidade temporária que é trocada a cada sessão;
- não-repúdio: esse serviço é utilizado para assegurar que o emissor de uma mensagem não negue posteriormente o que foi emitido ou até mesmo a sua participação em uma transação. O não repúdio é controlado pela existência da assinatura digital que somente pode ser gerada pelo emissor da mensagem.

3. MÉTODOS FORMAIS

Os protocolos estão sujeitos a ocorrência de erros em qualquer fase de seu projeto (especificação, construção e verificação). Por isso não é incomum que sejam descobertas falhas em protocolos publicados e utilizados por vários anos. Como exemplo, protocolo de (NEEDHAM e SCHROEDER, 1978) foi utilizado durante 4 anos até que (DENNING e SACCO, 1981) demonstraram que ele estava sujeito ao ataque do homem no meio e propuseram um protocolo alternativo. Porém, em 1994 Abadi e Needham demonstraram que este protocolo também possuía falhas (BUTTYÁN, 1999).

O emprego de métodos formais na área de criptografia é recente. Grande parte dos trabalhos nesta área são desenvolvidos na década de 90 (MEADOWS, 1995). Estes métodos permitem fazer uma análise completa do protocolo criptográfico e sua função principal é especificar se os objetivos propostos pelos autores são alcançados. Muitas vezes um protocolo é construído para realizar a distribuição segura de uma chave de sessão e quando analisado verifica-se que essa meta não é atingida.

Existem 4 abordagens diferentes para a análise de protocolos criptográficos (RUBIN e HONEYMAN, 1993), (MEADOWS, 2000) e (GRITZALIS, SPINELLIS e GEORGIADIS, 1999). A primeira é a menos popular enquanto que a terceira é a mais utilizada:

1. uso de linguagens de especificação e ferramentas de verificação: o objetivo principal desta abordagem é tratar um protocolo criptográfico como qualquer programa e tentar provar sua corretude. O principal problema é que estes métodos não são específicos para a análise de protocolos de segurança. Dentre os métodos podem ser destacados: LOTOS (*Language of Temporal Ordering Specification*) e *Ina Jo*. (VARADHARAJAN, 1990) utilizou LOTOS para analisar alguns protocolos criptográficos, porém não conseguiu demonstrar qualquer resultado. O autor concluiu que essa ferramenta não era adequada para a análise de segurança. Em (KEMMERER, 1989) é encontrada uma fraqueza no *Ina Jo*.
2. uso de sistemas especialistas: nestes métodos a maioria dos protocolos são modelados como máquinas de estado. São exemplos: *Interrogator* e NRL *Protocol Analyzer*. Neles o projetista especifica um estado inseguro e através de pesquisas exaustivas, tenta construir um caminho para este estado. Eles obtiveram mais êxito do que os anteriores, porém, possuem como desvantagem a grande quantidade de possíveis eventos que devem ser examinados;
3. uso de modelos baseados em lógicas modais: estas abordagens analisam os conceitos de crença e de conhecimento dos participantes do protocolo criptográfico. São utilizados principalmente para os protocolos de autenticação e de distribuição de chaves. Dentre eles pode-se destacar: as lógicas BAN e GNY. Apesar de serem mais simples e intuitivas do que as outras abordagens, são eficazes. O artigo da lógica BAN encontrou vários erros e redundâncias em protocolos bastante utilizados. Porém, o analista deve ter cuidado, pois suposições incorretas podem conduzir a erros na análise;
4. uso de sistemas algébricos: nesta abordagem o protocolo criptográfico é modelado como um sistema algébrico, associando um estado como se fosse o conhecimento do participante. São complementares aos métodos de lógica modal, pois também realizam uma formalização de problemas por hipóteses e nas propriedades de autenticação. O primeiro trabalho nesta área é o de Dolev-Yao e os outros trabalhos desenvolvidos são versões estendidas desse modelo. O problema desses sistemas é que são restritos para a análise da maioria dos protocolos. Só podem ser utilizados para descobrir fraquezas de segredos e não permitem que os participantes se lembrem de informações de um estado para o próximo.

O custo-benefício em utilizar uma dessas abordagens, antes de publicar o protocolo, é melhor do que ter que fazer alterações posteriores, já que é mais barato usar os métodos no desenvolvimento do protocolo do que fazer o seu replanejamento.

3.1. LÓGICA BAN

A lógica BAN foi desenvolvida por Burrows, Abadi e Needham (por isso o nome) em 1989. É a primeira lógica a analisar formalmente os protocolos criptográficos, principalmente os de autenticação e distribuição de chaves (BURROWS, ABADI e NEEDHAM, 1990).

É a lógica mais popular na literatura para a análise de crenças e de conhecimento entre os participantes dos protocolos criptográficos.

Apesar das críticas recebidas ela encontrou erros em vários protocolos, como o de Needham-Schroeder, CCITT X.509, Yahalom e Kerberos. A lógica BAN também é utilizada como validação dos protocolos propostos em (AZIZ e DIFFIE, 1994) que desenvolveram um protocolo de autenticação para o ambiente celular e em (MYRVANG, 2000) que desenvolveu um protocolo de autenticação para redes locais sem fio.

Outras lógicas começaram a ser desenvolvidas estendendo ou aplicando os mesmos conceitos da lógica BAN. A de maior sucesso entre elas é a GNY (GONG, NEEDHAM e YAHALOM, 1990).

A lógica GNY introduziu novos conceitos, como reconhecimento e posse de fórmulas e a expressão "não-originada-aqui" que permite aos participantes detectar mensagens que foram enviadas em sessões anteriores.

Porém, a lógica GNY é mais complexa, possui muitas regras (mais de 50) que devem ser aplicadas em cada fase do protocolo e mais difícil de ser utilizada. Alguns autores consideram-na impraticável (GRITZALIS, SPINELLIS e GEORGIADIS, 1999) e (SYVERSON e CERVESATO, 2000). A complexidade é o maior problema das lógicas estendidas da BAN.

Na dissertação de mestrado (SANTOS, 2002) foi realizada uma comparação entre as duas lógicas, chegando-se à conclusão que a lógica GNY, por conter muitas regras, pode tornar a análise mais suscetível a erros e redundâncias. A lógica BAN também consegue chegar nos mesmos resultados finais, além disso, ela é mais simples e mais fácil de aplicar e de empregar seus postulados. Por estes motivos, a autora decidiu utilizar a lógica BAN, para analisar três importantes protocolos de autenticação da rede celular: GSM (*Global System for Mobile Communications*), CDPD (*Cellular Digital Packet Data*) e UMTS (*Universal Mobile Telecommunications System*).

Como a lógica BAN possui muitos símbolos, a autora utilizou uma versão mais intuitiva que será mantida neste trabalho. Por exemplo, a expressão:

$P \models Q \mid\sim \#(X)$ é substituida por
P **acredita** Q **disse novo**(X) (lê-se: P acredita que Q, há algum tempo, disse que X é nova).

As principais expressões da lógica BAN são:

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. $\{X\}_K$: fórmula X cifrada com a chave K. As mensagens cifradas somente são legíveis e verificáveis pelo possuidor da chave.

A notação abaixo é usada numa troca de mensagem:

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.

3.1.1. POSTULADOS LÓGICOS

Da mesma forma que na notação básica, será utilizada uma representação mais compreensível dos postulados (ou regras). Os principais postulados utilizados neste trabalho são:

B1. Regra de significado da mensagem:

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

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.

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. Uma descrição mais detalhada e exemplos da lógica BAN podem ser encontrados em (BURROWS, ABADI e NEEDHAM, 1990) e (SANTOS, 2002).

4. ANÁLISE FORMAL DOS PROTOCOLOS

Nesta seção será apresentada uma breve descrição, a análise formal dos protocolos de autenticação: GSM, CDPD e UMTS e uma comparação entre eles.

Além da comparação dos três protocolos, 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, validando o trabalho de Godfrey e a certeza das fraquezas encontradas nos dois protocolos. Outra diferença é que a sexta mensagem do protocolo do GSM é considerada na análise já que faz parte dos serviços de segurança (sigilo da identidade do usuário). Este trabalho também analisa o protocolo de autenticação do UMTS que não foi realizada em Godfrey.

4.1. 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

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

4.1.1. 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) e (MOULY e PAUTET, 1992):

- autenticação da identidade do assinante: o assinante tem que provar sua identidade ao sistema antes de realizar qualquer transação. 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. Ela é trocada a cada sessão, evitando que um intruso consiga obter uma chave durante a execução atual do protocolo e tente utilizá-la em comunicações posteriores.

Devido a mobilidade, existe uma grande possibilidade do terminal móvel (A) requerer serviço num outro domínio que não seja a da sua rede domiciliar (C). Neste caso, a rede servidora (B) 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. 1).

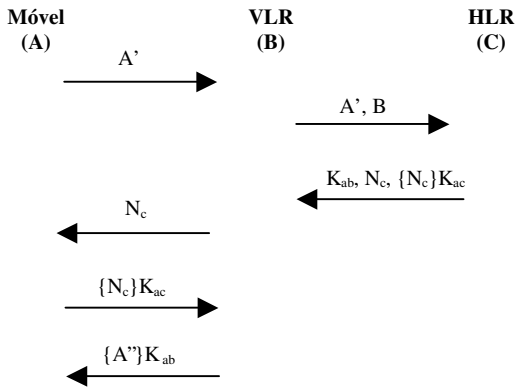

FIG. 1 – Protocolo de Autenticação do GSM
(móvel fora da área de registro)

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 a autenticação é realizada com sucesso. Caso contrário, a conexão é liberada e um aviso é enviado ao móvel;
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.

4.1.2. ANÁLISE FORMAL

Nesta seção é realizada a análise formal do protocolo de autenticação GSM. Primeiro será mostrado como as mensagens são transferidas entre os participantes do protocolo. Depois o protocolo é transformado numa forma idealizada, são realizadas as suposições e aplicados os postulados da lógica BAN chegando-se nas conclusões.

- 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

Como a lógica BAN não cosidera as mensagens em texto em claro, já que acredita que elas podem ser forjadas por um intruso e não contribuiriam para a análise, então, as duas primeiras mensagens não são utilizadas. A terceira, apesar de estar em texto em claro, é considerada já que o sistema GSM confia na segurança do enlace cabeado.

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	$B \rightarrow A$	$\{\textbf{novo}\ A\}K_{ab}$

- 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** ($A \overset{K_{ab}}{\longleftrightarrow} B$, N_c, $\{N_c\}K_{ac}$, **novo**$\{N_c\}_{K_{ac}}$) (9)

B **acredita** ($A \overset{K_{ab}}{\longleftrightarrow} B$, N_c, $\{N_c\}K_{ac}$, **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** $A \overset{K_{ab}}{\longleftrightarrow} B$ (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** $A \overset{K_{ab}}{\longleftrightarrow} B$ (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 GSM transmite o número aleatório 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 na rede.

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.

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 A. Se a resposta ao desafio for igual ao valor recebido na terceira mensagem, então o móvel 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, atendendo o requisito de segurança: 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** $A \overset{K_{ab}}{\longleftrightarrow} B$	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.

Independente da utilização da lógica BAN, é encontrado outro problema com os serviços de segurança no GSM já 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.

4.2. 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).

4.2.1. 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}.

Para o fluxo de mensagens mostrado na FIG. 2, supõe-se que o terminal móvel está fora da sua área de registro.

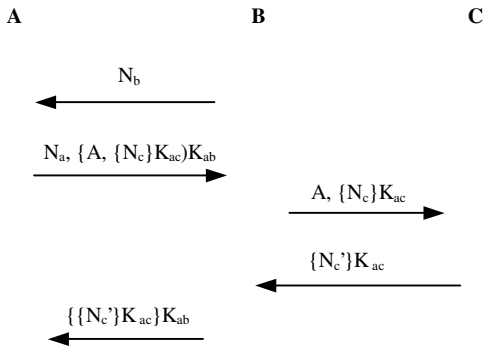

FIG. 2 – Protocolo de Autenticação do CDPD

O processo inicia com a troca de chaves Diffie-Hellman 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 também calcular K_{ab}. 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 RC-4 (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.

4.2.2. 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	$B \rightarrow A$	$A \overset{N_b}{\longleftrightarrow} B$

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

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 $\overset{N_b}{\longleftrightarrow}$ B
2. B **acredita** A **controla** A $\overset{N_a}{\longleftrightarrow}$ B
3. B **acredita** A **acredita** A $\overset{N_a}{\longleftrightarrow}$ B
4. A **acredita** B **acredita** A $\overset{N_b}{\longleftrightarrow}$ B
5. A **acredita** B **disse** N_b
6. B **acredita** A **disse** N_a
7. C **acredita** A $\overset{K_{ac}}{\longleftrightarrow}$ C
8. A **acredita** A $\overset{K_{ac}}{\longleftrightarrow}$ 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 $\overset{N_b}{\longleftrightarrow}$ B (12)

A **acredita** B **acredita** A $\overset{N_b}{\longleftrightarrow}$ B (4)

A **acredita** B **controla** A $\overset{N_b}{\longleftrightarrow}$ B (1)

A **acredita** A $\overset{N_b}{\longleftrightarrow}$ 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 A e B.

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

Mensagem 2:

B **recebeu** (A $\overset{N_a}{\longleftrightarrow}$ B, $\{\{N_c\}K_{ac}\}K_{ab}$) (14)

B **recebeu** (A $\overset{N_a}{\longleftrightarrow}$ B) (15 - B4, 14)

B **recebeu** ($\{\{N_c\}K_{ac}\}K_{ab}$) (16 - B4, 14)

B **acredita** A **controla** A $\overset{N_a}{\longleftrightarrow}$ B (2)

B **acredita** A **acredita** A $\overset{N_a}{\longleftrightarrow}$ B (4)

B **acredita** A $\overset{N_a}{\longleftrightarrow}$ 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 $\overset{K_{ab}}{\longleftrightarrow}$ B (18)

B **acredita** A $\overset{K_{ab}}{\longleftrightarrow}$ 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 recebe a fórmula (16) e gera a chave de sessão, a partir da combinação dos números aleatórios (N_a e N_b). Depois aplica a regra (B1) nas fórmulas (16) e (19) obtendo a fórmula (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 recebe 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) aplica a regra (B1) em (27) e (18) e obtém (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** $A \overset{K_{ab}}{\longleftrightarrow} B$

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

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 só consegue atingir os objetivos da autenticação do terminal móvel e de distribuição da chave de sessão 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*.

4.3. 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. 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).

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 (YACOUB, 1993). O novo sistema 3G-UMTS já está sendo introduzido na Europa e na Ásia.

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. 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 de ciframento, além de outras informações relacionadas ao assinante (BARBA, CRUSELLES e MELÚS, 1993).

4.3.1. 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 (RAMASAMI, 2000).

- sigilo da identidade do assinante: é realizado pelo uso de identidades temporárias (TMUI – *Temporary Mobile User Identity*) com validade local. 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 GSM).

O protocolo de autenticação proposto é baseado no sistema criptográfico de chave simétrica. Ela possui somente três mensagens trocadas entre o móvel (A) e a rede servidora (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. 3).

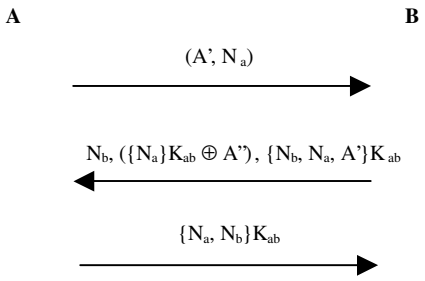

FIG. 3 – Protocolo de Autenticação do UMTS

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, decifra {N_b, N_a, A'} com a chave secreta compartilhada com B e obtém o número aleatório N_b que será comparado 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 um algoritmo para geração de chaves de sessão, onde as entradas são N_a, N_b, A" cifradas com a chave secreta K_{ab}.

4.3.2. ANÁLISE FORMAL

- Protocolo

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

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

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

- Suposições

1. A **acredita** $A \overset{K_{ab}}{\longleftrightarrow} B$
2. B **acredita** $A \overset{K_{ab}}{\longleftrightarrow} B$
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} ⊕ A")
8. A **acredita novo**({N_a}K_{ab} ⊕ 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} ⊕ A"), {N_a, N_b}K_{ab} (11)

A **recebeu** N_b (12 - B6, 11)

A **recebeu novo**({N_a}K_{ab} ⊕ 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), aplica a regra (B6) e encontra as fórmulas (12), (13) e (14). Utilizando a regra (B1) em (14) e (1) 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 4.3.1, ou seja, a autenticação mútua, a distribuição da chave de sessão e o sigilo da identidade e dos dados do assinante. 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 possa ser aproveitada por um intruso.

Para complementar a análise e confirmar a segurança é importante que seja empregado algum método de criptoanálise e, dessa forma, verificar a força do algoritmo e analisar os ataques que o protocolo ou os seus algoritmos estão sujeitos. Se um intruso, por exemplo, conseguir obter a chave secreta K_{ab}, poderá se passar por um assinante ou uma estação base legítima e ter acesso a todas as informações.

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.

Dos três protocolos de autenticação analisados, somente o UMTS mostrou fornecer os serviços desejados.

5. CONCLUSÃO

Este trabalho mostrou 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.

Todavia deve-se 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, como mostrado no GSM e no CDPD.

Neste trabalho foram realizadas as avaliações de três protocolos do ambiente de comunicação celular. Também foi sugerida e empregada uma notação mais compreensível da lógica BAN, além da análise do protocolo de autenticação do UMTS e de uma comparação entre os três protocolos que não haviam sido realizadas.

REFERÊNCIAS BIBLIOGRÁFICAS

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

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. Nova Jersey. Outubro 1993.

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.**

http://citeseer.nj.nec.com/context/1960161/0**.** Technical Report SSC/. Novembro 1999.

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.

DORNAN, Andy. **The Essential Guide to Wireless Communication**. Prentice Hall PTR. 2001.

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

GODFREY, James. **A Comparison of Security Protocols in a Wireless Network Environment**. Dissertação de Mestrado. Universidade de Waterloo. Canadá – 1995. 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.

JOSEPH, Anthony D. **Privacy and Security in Wireless Networks**. 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.

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

MEADOWS, Catherine. **Formal verification of cryptographic protocols: A survey**. ASIACRYPT'94 , 133-150, http://citeseer.nj.nec.com/134868.html. 1995.

MEADOWS, Catherine. **Open Issues in Formal Methods for Cryptographic Protocol Analysis**. DISCEX 2000:, 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.

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

MYRVANG, Per Harald. **An Infrastructure for Authentication, Authorization and Delegation**. 2000. Tese, Universidade de Troms∅, Faculdade de Ciência, 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.

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

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

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

SANTOS, Myrna C. M dos. **Análise Formal de Protocolos de Autenticação para Redes Celulares**. Dissertação de Mestrado. Instituto Militar de Engenharia, 2002.

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

SYVERSON, Paul e CERVESATO, Iliano. **The Logic of Authentication Protocols**. FOSAD´00. Setembro 2000.

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

YACOUB, Michel Daoud. **Foundations of Mobile Radio Engineering**. CRC Press, Inc., 2000 Corporate Blvd. P. 481. 1993.